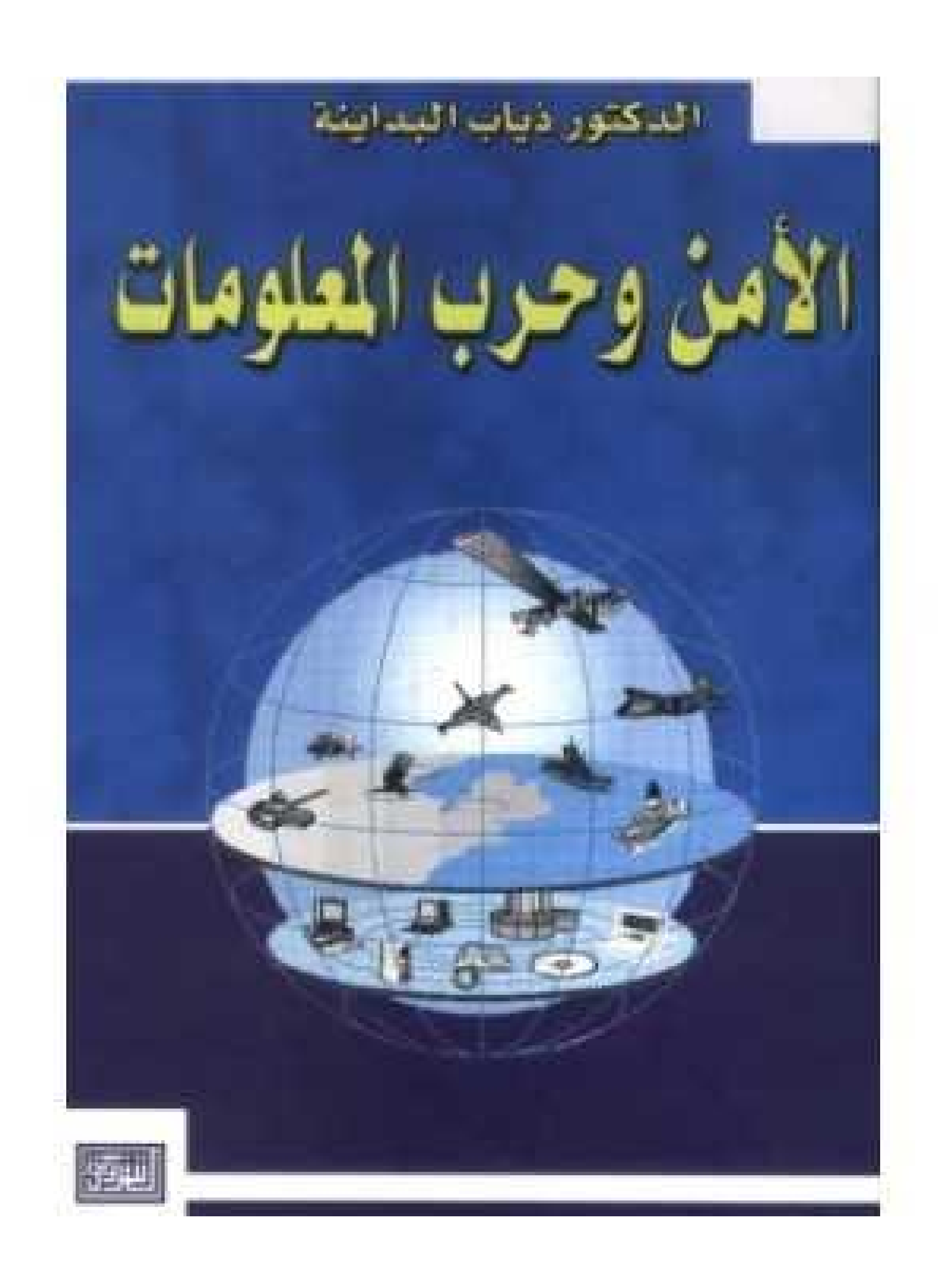


الأمن وحرب المعلومات

المؤلف: د.ذياب البداينة

الناشر: دار الشروق

في المجتمع المعلوماتي تحول العالم لى بيت عنكبوت غير منظم الروابط عالم الشبكات والصفر والواحد موصول بطرق افتراضية فائقة السرعة

المحتويات

جدول المحتويات ـــــ أ-ح
فهرس الجداول ـــــ ك
فهرس الأشكال ـــــ ل
المقدمة ـــــ 5

الجزء الأول: الأمن في المجتمع المعلوماتي

تمهيد ـــــ 12
الفصل الأول: الأمن الوطني في المجتمع المعلوماتي: المفهوم والتحديات والانكشافات ـــــ 13
مقدمة ـــــ 14
الأمن : المفهوم ـــــ 21
الأمن من المنظور المعلوماتي ـــــ 22
تحديات المجتمع المعلوماتي ـــــ 23
الفصل الثاني: الثغرات الأمنية الجديدة والتهديدات المشتركة ـــــ 29
مقدمة ـــــ 31
التهديدات ـــــ 33
الثغرات (الانكشافات) الجديدة ـــــ 34
1- قطاع الاتصالات والمعلومات ـــــ 37
2- قطاع التوزيع الفيزيقي ـــــ 39
3- قطاع الطاقة ـــــ 39
4- قطاع المال والبنوك ـــــ 40
5- قطاع الخدمات الانسانية الحيوية ـــــ 41
وسائل التعدي على البنية التحتيه المعلوماتية ـــــ 42
الفصل الثالث: خصائص المجتمع المعلوماتي ـــــ 47
مقدمة ـــــ 49

معايير المجتمع المعلوماتي 57
خصائص مجتمع المعلومات: 58
أولاً: الخصائص التقنية 71
ثانياً: الخصائص الاجتماعية 87
ثالثاً: الخصائص الثقافية 93
رابعاً: الخصائص السياسية 96
خامساً: الخصائص الاقتصادية 101
سادساً: الخصائص الأمنية 105
الأمن العربي في عصر المعلومات

الجزء الثاني: حرب المعلومات : التطور والنظرية

تمهيد 112
الفصل الرابع : تطور حرب المعلومات 113
مقدمة 114
تطور حرب المعلومات 115
المبادئ الجديدة للحرب في عصر المعلومات 126
مبادئ العدوان 128
مبادئ التفاعل 130
مبادئ السيطرة 131
مجالات حرب المعلومات: 132
أ- العبث (اللعب) 132
ب- الجريمة 136
ج- حقوق الفرد 140
د- الأمن الوطني 141
حرب المعلومات الاستراتيجية 149
خصائص حرب المعلومات الاستراتيجية 145
الفصل الخامس : حرب المعلومات: النظرية 151
مقدمة 153

مفهوم حرب المعلومات 153
نظرية حرب المعلومات: 164
أولاً: مصادر المعلومات 164
قيمة مصادر المعلومات 166
ثانياً: أطراف الصراع 170
ثالثاً: عمليات الهجوم 174
الاعداد والتصميم في حرب المعلومات 178
نمذجة حرب المعلومات 178
خطوات تنفيذ حرب المعلومات 181
الفصل السادس : حرب الخليج وأسلحة التخريب الشامل 185
مقدمة 187
1- تدمير البناء التحتي المعلوماتي 188
أ- تدمير نظم المعلومات 188
ب- شبكات الطاقة 189
ج- القنابل الكهرومغناطيسية 190
2- الوصول غير المصرح به للمعلومات 190
3- التجسس العسكري المعلوماتي 192
4- التجسس الالكتروني 194
5- زرع الفيروسات 196
6- العمليات النفسية 197
أ- التلفزيون والمحطات الفضائية 197
ب- الاذاعة 201
ج- الدعاية 202
د- المنشورات الورقية 203
هـ- الخداع 207
و- الخطابات 208
7- الرقابة الإعلامية 208

أ. الانتقاء الإعلامي 208
ب- المراقبة الاعلامية بالتأخير 210
ج- التنصت 210

الجزء الثالث: حرب المعلومات الهجومية

تمهيد 213
الفصل السابع : المصادر المفتوحة 215
مقدمة 217
المصادر المفتوحة: 217
1- استخبارات المصادر المفتوحة 217
2- المتصفحات 218
3- بروتوكول النص الفائق 218
4- تحميل البرامج المجانية 219
5- محركات البحث 219
6- البريد الالكتروني 219
7- بريد القمامه 219
8- التجارة الالكترونية 219
9- التفتيش في القمامة 220
10- الشمشمة 221
11- تصفح الوب 222
12- استغلال الملكية الفكرية 222
13- خرق الملكية الفكرية على الانترنت 223
14- خرق حقوق النشر 223
15- قرصنة البرامج 224
16- خرق حماية الاتصالات والبيانات 227
17- خرق الخصوصية 229
18- الكعكات 229

الفصل الثامن: العمليات النفسية وإدارة النفس والادراك 231
مقدمة 233
أنواع العمليات النفسية 234
مبادئ العلميات النفسية 235
إدارة النفس والادراك 236
وسائل الحرب النفسية المعلوماتية: 238
1- الكذب 238
2- التشويه 238
3- التحريف 239
4- الفسوق 239
5- الخداع 240
6- الهندسة الاجتماعية 241
7- الشجب 244
8- التحرش 245
9- الاعلان 246
10- الاحتيال المالي 246
11- بريد القمامة الالكتروني 247
12- الرقابة 247
13- التهديد الثقافي 248
14- التوهج 249
الفصل التاسع : الداخليون 251
مقدمة 253
1- الخونة والجواسيس 253
2- علاقات العمل 258
3- الزيارات والطلبات 258
4- الاحتيال والاختلاس 259
5- الصفقات المصطنعة 260

6- تعديل البيانات 260
7- التخريب الداخلي 260
8- الهجمات الفعلية 261
9- الهجمات البرامجية 261
10- انتحال صفة الآخرين 261
الفصل العاشر : مُصادرة الاشارات 263
مقدمة 265
اعتراض الاتصالات 265
1- التلفون 266
2- خدمات الهاتف 267
3- الجوال والبيجر 267
4- تسجيل المكالمات 269
5- الفاكس 270
6- التلفون اللاسلكي 270
7- آلة الرد الصوتي 270
8- البريدالصوتي 271
9- اعتراض الاستخبارات الاجنبية 271
10- حل رموز الرسائل 273
11- الارسال بالستالايت 274
12- الفيديو 276
13- التنصت على المحادثات الهاتفية 276
الاحتيال في الاتصالات الهاتفية 277
1- الاحتيال في البريد الصوتي 278
2- الاحتيال في بطاقات الاتصال 278
3- الاحتيال بالجوال والهواتف المقلدة 279
مراقبة شبكات الحاسب 279
1- شمامو الحزم المعلوماتية 280

2- مراقبة ادخال المفاتيح 280
3 - تحليل المرور الالكتروني 280
4- كلمات الدخول 281
5- المودم 282
6- الحرمان من الخدمة 283
المراقبة البيئية 284
1- الكاميرات والفيديو 284
2- الستالايت 284
3- لاقطات فان إيك 285
4- المجسات الاخرى 285
5- المراقبة من الكتف 286
الفصل الحادي عشر: الاختراق 287
مقدمة 289
أدوات الحصول على الدخول غير المصرح به وأساليبها 290
1- ماسحات الشبكات 290
2- رزم الشم 291
3- مروجو كلمات المرور 291
4- الهندسة الاجتماعية 291
5- سرقة المعلومات 292
6- جمع التذكار 292
7- التأثير 293
8- تتبع الموقع على الشبكة 293
9- الغلق عن بعد 294
التخريب 295
1- التشويش 295
2- بنادق اتش أي آر آف 296
3- قنابل تحويل النبضات الكهرومغناطيسية 296

4- اسلحة ترددات الراديو 297
5- اسلحة الموجات القصيرة 298
الفصل الثاني عشر : التنكر والخفاء 299
مقدمة 301
سرقة البطاقة (الهوية) 301
الرسائل والوثائق المزورة 302
1- تزوير البريد الالكتروني 302
2- التزوير في البريد الدعائي 303
3- الفيضانات البريدية 303
4- تغير العنوان 304
5- التزييف 304
حصن طروادة 305
1- برمجيات حصن طروادة 305
2- ركوب الوب 306
3- تتبع البريد الالكتروني 306
الفصل الثالث عشر : الوباء الالكتروني 307
مقدمة 309
الفيروسات 309
1- فيروسات قطاع التشغيل 311
2- فيروسات الماكرو 312
3- الفيروسات الطفيلية 312
4- فيروسات البرامج 312
ديدان الانترنت 313
حصن طروادة 313
القنبلة المنطقية 314

الجزء الرابع : حرب المعلومات الدفاعية

تمهيد —— 317

الفصل الرابع عشر : سد الثغرات والانكشافات —— 321

مقدمة —— 323

مراقبة الانكشافات —— 323

أنواع التهديدات —— 324

ايجاد الثغرات في الحاسب والشبكات —— 325

مراقبة المنشورات الأمنية —— 326

بناء النظم الآمنة —— 327

الوعي الأمني والتدريب —— 328

تجنب الانهيار الكلي —— 328

إدارة الخطورة —— 329

1- تحليل الخطورة —— 329

2- تحديد التهديدات —— 330

3-تقدير الخطورة —— 332

الدفاع عن المجتمع المعلوماتي —— 332

البناء الوطني المعلوماتي —— 332

حماية البنية التحتية الوطنية المعلوماتية —— 334

1- المبادئ العامة —— 335

2- الهيئة الرئاسية —— 337

سياسة التشفير —— 342

أ- صنع الترميز —— 343

ب- فك التشفير —— 343

ج- فحص التشفير وقوته —— 344

السياسة الدولية في التشفير —— 344

التهديدات الخارجية —— 345

الفصل الخامس عشر : مخابئ المعلومات 347
مقدمة 349
1- الحماية الفيزيقية 349
وسائل الحماية الفيزيقية 350
أ- العوائق 350
1- المفاتيح والاقفال 350
2- الحماية من الكوارث الطبقية 351
3- الحماية من التهديدات البيئية 351
ب- ضبط الدخول 351
ج- المراقبة 352
1- التفتيش المنتظم 352
2- التفتيش العشوائي 352
3- اختبارات الدخول غير المصرح بها 353
انموذج للحماية الفيزيقية للمعلومات 353
2- التشفير (التعمية) 354
نظام التشفير الرقمي 356
فك الشفرة 357
توليد وتوزيع المفاتيح 357
تشفير المفتاح العام أر اس ايه 359
1- التشفير بالمفتاح العام 359
2- طريقة أر اس ايه 360
3- توزيع المفاتيح العامة 361
4- التشفير بالمفتاح السري 362
نظام المفتاح الخاص 363
رقيقة كليبر 365
قصور التشفير 365
المخابئ 365

المجهولية 366
الترشيح 367
6- التخلص من النفايات المعلوماتية 368
7- درع المعلومات 368
الفصل السادس عشر: نقاء المعلومات 371
مقدمة 373
1- التحقق من الأمن الفيزيقي 373
2- وسائل الكشف والاثبات البيولوجية الاحصائية 374
3- قياسي التكاملية 375
4- التوقيع الرقمي 375
5- كلمات المرور والمتعلقات السرية الأخرى 375
6- إدارة المفاتيح العامة والشهادات 376
7- العلامات المائية 376
8- الاتصال الراجع والاتصال بالمنزل 377
9- التحقق بناءً على الموقع 377
10- الشارات والبطاقات 378
الفصل السابع عشر : حراسة المعلومات ورقابتها 379
مقدمة 381
1- التحكم بالدخول للأصول المعلوماتية 381
أ- سياسات السماح بالدخول 381
ب- رقباء التحكم في الدخول 384
2- ترشيح المعلومات 387
أ- جدران الحماية 387
ب- مرشحات البريد غير المرغوب 388
ج- مرشحات الشبكة 389
3- اكتشاف التطفل وسوء الاستخدام 390

أ- الرقابة في مكان العمل ____ 391
ب- الكشف التلقائي ____ 392
ج- خرق الحاسب وكشف سوء الاستخدام ____ 392
المراجع ____ 395
أ- العربية ____ 395
ب- الانجليزية ____ 402
الملاحق ____ 463

فهرس الجداول

جدول رقم (1) التطورات في التقنيات الكونية. ____ 66
جدول رقم (2) مقارنة خصائص المجتمع الصناعي
مع خصائص المجتمع المعلوماتي. ____ 75
جدول رقم (3) مقارنة بين النماذج القياسية والنماذج الفنية الاجتماعية. ____ 77
جدول رقم (4) ثلاثية النهايات والمابعديات والمنفيات "بلا". ____ 79
جدول رقم (5) الموضوعات التقنية والمشكلات الاجتماعية. ____ 85
جدول رقم (6) المهن البينية في المجتمع المعلوماتي. ____ 100
جدول رقم (7) حجم الخسارة المالية للتعديات على
امن المعلومات للفترة من 1997-1999م. ____ 104
جدول رقم (8) مؤشر نصيب الفرد من وسائل المعلومات والاتصال. ____ 106
جدول رقم (9) قيمة الانفاق على البحث العلمي والتطوير في العالم ونسبة
الانفاق في الدول المتقدمة والنامية والعربية. ____ 107
جدول رقم (10) حجم الاستخدام على الشبكة وفق اللغة حزيران2001م. ____ 108
جدول رقم (11) محتوى الشبكة وفق اللغة لعام 2001م. ____ 109
جدول رقم (12) توزيع مستخدمي الانترنت وفق المناطق. ____ 109
جدول رقم (13) انموذج الموجات الثلاث. ____ 162
جدول رقم (14) موضوع المنشورات وفق الحجم. ____ 206
جدول رقم (15) تقديرات قرصنة برمجيات الحاسب لعام 1994م. ____ 225

فهرس الاشكال

شكل رقم (1) مستويات الامن في المجتمع المعلوماتي ـــــــ 27
شكل رقم (2) توزيع عمالة المجتمع الامريكي بين القطاعات المختلفة. ـــــــ 55
شكل رقم (3) مبادئ الحرب في عصر المعلومات. ـــــــ 120
شكل رقم (4) العمليات الهجومية والدفاعية في حرب المعلومات. ـــــــ 146
شكل رقم (5) الوظائف الفرعية الخمس ـــــــ 354
شكل رقم (6) تسلسل عملية التشفير باستخدام مزدوج للمفتاح العام والخاص ـــــــ 362

الملاحق

ملحق (أ) ـــــــ 463
مرجع الخنجر العسكرية السويسرية
مصادر في أدوات المعلومات والأمن

المقدمـــة

في المجتمع المعلوماتي، تحول العالم إلى بيت عنكبوت غير منظم الروابط، عالم الشبكات و الصفر والواحد، موصول بطرق افتراضية وفضائية فائقة السرعة. عالم توحدت فيه البنى التحتية المعلوماتية على المستويات الوطنية والإقليمية والدولية لتصبح بنية معلوماتية كونية. عصر وصلت التطورات الرئيسة (كما وصفها كاكو، 2001) في أعمدة العلم الثلاثة : المادة، والحياة، والعقل (الذرة، والـ D.N.A، والحاسب) إلى قمتها. عصر اصبح الخيال العلمي واقعاً ، لابل أصبح من الصعب احياناً التمييز بين الواقع والخيال والافتراض. عصر تغيرت فيه قواعد اللعب السياسية، عصر يُشكل ويعاد تشكيله بسرعة. عصر «تفصيل البشر» كما تشاء على شكل نخبة، وعمال، وجنود، عصر حروبه بلا جيوش، وبلا دماء، عصر استبدل فيه الرصاص بالبايتات. عصر تشكل المعلومات الأساس الأهم فيه للأعمال والأمن ولكل شيء.

عصر لم تعد الحكومات ولا الدول تخشى من بعضها البعض بقدر خشيتها من المنظمات، والجماعات والأفراد، عصر أصبح فيه تصريح أو مقابلة تلفزيونية مع أحد قادة المنظمات (الإرهابية) يجعل من الولايات المتحدة القوة الأوحد في العالم تعلن حالة التأهب في قواتها في كثير من المناطق، وشخص أو مجموعة أشخاص يغلقون مكاتب الكونجرس الامريكي بسبب مخاوف انتشار الرسائل الملوثة بالجمرة الخبيثة. وتسبب مجموعة من الافراد في تكوين تحالف دولي (ضد الإرهاب) وشن حرب بكلفة مليارات الدولات على افغانستان وغيرها في الوقت الذي كانت حفنة من الدولات تنقذ حياة عائلة أفغانية. وهذه الولايات المتحدة تشن حرباً كونية على أفراد مثل أسامة بن لادن، والملا عمر وطالبان في افغانستان بعد حادث تدمير برج التجارة الدولية وتدمير جزء من البنتاغون في عمليات استخدمت فيها طائرات مدنية مختطفة وتم تفجير هذه المباني بواسطتها، (فيما عرف بأحداث 11/9/2001) ادت هذه العمليات إلى اختفاء الرئيس ونائبه خوفاً من استهدافهما. والولايات المتحدة اذ تدمر جبالاً مثل تورا بورا بأكملها وتلقي أكثر القنابل دماراً وقتلاً بحثاً عن مجموعة افراد.

إن الموازنه الامريكية كما صرح الرئيس الامريكي جورج بوش ستواجه عجزا هذا العام بسبب هذه الحرب. لقد أصبحت محاولة تعقب المجموعات غير المرغوب فيها من الصعوبة بمكان، لا بل إن قدرة الدولة على ضبط الناس، والتحكم بهم قد أصبحت ضعيفة وستزداد ضعفاً يوماً بعد يوم. فهذه بعض المواقع التي تعرض مواد لاترغب بها بعض الدول تقوم الاجهزة الأمنية بحجبها عن المجتمع بكامله. ولكن ومن خلال مواقع أخرى مصممة لكسر مثل هذا الحجب مثل (Silent Surfأو، www.megaproxy.com) والتي استخدمت للدخول لموقع مثل موقع عرب تايميز (www.arabtimes.com)، حيث يقوم هذا الموقع بنشر معلومات غير مرغوبة في بعض الدول، لا بل تشكل فضائح في بعضها؛ حيث لا سلطة لمقص الرقابة عليها. وعلى المستوى السياسي فهذا الشاه رابع أكبر قوة عسكرية يهزمه آية الله الخميني بثورة الكاسيت، وهذه أحزاب المعارضة تهرب للخارج، وتقاتل في الداخل من خلال الفاكس، والبريد الإلكتروني، والصحف، والقنوات الفضائية، لا بل إن الأطفال قد يعطلون دفاعات وزارة الدفاع الأمريكية الأكثر تحصيناً، من خلال بعض برمجيات التلصص، والقرصنة، والفيروسات... الخ المتاحة على الانترنت.

وإذا كان من عامل مشترك لكل هذه التحديات فإنه يمكن تلخيصه بكلمة واحدة هي كلمة "المعلومات". المعلومات مصدر نادر وهام، سلاح هجوم وسلاح دفاع. فمعرفة المعلومات عن الخصم ذات قيمة لاتقدر بثمن في وقت الازمات والحروب. فمثلا وصلت قيمة المعلومات التي تفضي إلى اعتقال بعض قادة تنظيم القاعدة إلى ملايين الدولات. وتدفع الدول والمنظمات والشركات ملايين الدولارات لقاء نقل معلومات استخبارية او تجسس تتعلق بالصناعة أو الاقتصاد. لقد طفت أسئلة كثيرة عقب تفجيرات نيويورك وواشنطن تركزت حول الاستفسار عن دور ال CIA، وال FBI، في تقديم المعلومات التي كان يمكن إن تجنب مثل هذه التفجيرات. لقد بينت هذه التفجيرات أن أمن أقوى دولة ليس بمحصن ضد التهديد ليس من الاعداء التقليديين مثل روسيا أو الصين أو من الدول «المارقة»، وانما من مهددات جديدة يمكن إن تكون عن بعد (من الخارج) او من الداخل من افراد أو مجموعة افراد. أو من مجموعة بسيطة دكت اقوى رموز القوة الاقتصادية والعسكرية في العالم وببث مباشر أمام العالم وأغلقت مكاتب الكونجرس الامريكي ونشرت الذعر لدى المجتمع الامريكي بنشر بكتيريا الجمرة الخبيثة.

يتناول هذا الكتاب الأمن في المجتمع المعلوماتي، وخصائص مجتمع المعلومات وحرب المعلومات، ويغطي مجالات كثيرة في هذا الموضوع، حيث شمل الأمن في المجتمع المعلوماتي، والتحديات التي تواجهه في هذا المجتمع، كما ركز على خصائص المجتمع المعلوماتي، وعمليات حرب المعلومات الهجومية، والدفاعية، وأمثلة وتطبيقات لحرب المعلومات وخاصة حرب الخليج الثانية. ولقد تطورت فكرة هذا الكتاب من خلال العديد من القراءات في هذا المجال، ومن المشاركات العملية في الندوات والدورات العلمية في أكاديمية نايف العربية للعلوم الأمنية أثناء عملي فيها خلال الفترة (1996-2001م). ولقد تأثرت كثيراً، واستفدت كثيراً مما كتبته دورثي داينج (Dorothy E. Denning) وهي من أعلام حرب المعلومات، ومن كبار المختصين في هذا المجال، كما إن لمنشورات عالم المعرفة الصادرة من الكويت مساهمة كبيرة في تطوير الكثير من الأفكار، والاطلاع على الحديث من التطورات في المجالات ذات العلاقة، وخاصة رؤى مستقبلية لميتشيو كاكو (ترجمة سعد الدين خرفان)، وثورة الانفوميديا لفرانك كيلش (ترجمة حسام الدين زكريا)، والعرب في عصرالمعلومات تأليف نبيل علي، وما بعد الإنترنت تأليف بيل جيتس (ترجمة :عبد السلام رضوان).

يركز هذا الكتاب كثيراً على ماذا نعرف عن المجتمع المعلوماتي وحرب المعلومات أكثر مما يركز على كيف نصنع حرب معلومات، إلا أنه شمل الكثير من التطبيقات العملية في هذا المجال.

يتكون هذا الكتاب من أربعة أجزاء شملت سبعة عشر فصلاً. عُني الجزء الأول بالأمن في المجتمع المعلوماتي، ويتكون من ثلاثة فصول. تناول الفصل الأول الأمن الوطني في المجتمع المعلوماتي، وشكل هذا الفصل تقديماً للأمن في المجتمع المعلوماتي من حيث المفهوم، والتحديات الأمنية في المجتمع المعلوماتي. تناول الفصل الثاني الثغرات الجديدة، والتهديدات الأمنية المشتركة، والتي شملت الثغرات المتعلقة بالاتصالات، والمعلومات، والتوزيع الفيزيقي، والطاقة، والمال، والبنوك، والخدمات الإنسانية الحيوية، والتهديدات لكل من هذه الثغرات، والانكشافات. أما الفصل الثالث فتناول معايير المجتمع المعلوماتي، وخصائص مجتمع المعلومات التقنية (كالمعلوماتية، والتخيلية "الافتراضية"، والرقمنة، والتقنية، والفضائية (السبرناتية)،

والاتصالات)، والاجتماعية (كالمعلوماتية الاجتماعية، والتغير الاجتماعي، والشبكات الاجتماعية، والحراك الحر، والتغير المعلوماتي، والتفاعل التخيلي، والتفاعل عن بعد)، والاقتصادية (كالاقتصاد الإلكتروني، والمهن الإلكترونية)، والسياسية (اللاحدود، والحكومة الإلكترونية)، والثقافية (الثقافة الكونية، والعولمة)، والأمنية (أمن المعلومات، والجرائم الفضائية)، كما تناول الأمن العربي في عصر المعلومات.

تناول الجزء الثاني حرب المعلومات: التطور والنظرية، حيث ركز الفصل الرابع على حرب المعلومات عامة من حيث المفهوم، والتطور، والأسس التي تقوم عليها، ومجالاتها. أما الفصل الخامس فتناول النظرية، حيث تم استعراض نظرية داينيج في حرب المعلومات، واستعراض أنموذج مختصر لتقييم حرب المعلومات. كما تناول الفصل السادس بعض التطبيقات العملية لحرب المعلومات، وخاصة ما تم استخدامه في حرب الخليج من أساليب، ووسائل، وأدوات.

أما الجزء الثالث فتناول حرب المعلومات الهجومية، حيث ركز الفصل السابع على المصادر المفتوحة كوسائل هجومية في حرب المعلومات بما في ذلك الاستخبارات والإنترنت، والأسرار التجارية، والقرصنة للبرمجيات. أما الفصل الثامن فتناول بالتفصيل العمليات النفسية، وإدارة الإدراك النفسي. كما تناول أنواع العمليات النفسية، ومبادئها ووسائلها (كالكذب، والتحريف، والتشويه، والهندسة الاجتماعية . . . إلخ). وتناول الفصل التاسع الداخليون، وخاصة الخونة والجواسيس، والجواسيس العسكريون، والتجسس الإلكتروني، والاقتصادي، والتجسس المؤسسي، وعلاقات العمل، والزيارات والطلبات. أما الفصل العاشر فتناول أساليب الاعتراض الفضائي للمعلومات، والإشارات، والموجات من كافة وسائل الاتصال، والبث، والنقل كالتلفونات، والستالايت، والتسجيل، والفاكس، والتلفون النقال، واللاسلكي، والبريد الصوتي، والبريد الإلكتروني. في حين تناول الفصل الحادي عشر الاختراقات، وشمل اختراق الحسابات، والوصول إلى المواقع وأدواته (ماسحات الشبكة، ورزم الشم، والهندسة الاجتماعية . . . إلخ). ويتناول الفصل الثاني عشر التنكر والخفاء، وشمل الاختفاء من خلال سرقة البطاقات، واستخدام الرسائل والوثائق المزورة (مثل تزوير البريد الإلكتروني، والفيضانات، والبريد الدعائي،

والتزييف). ويتناول الفصل الثالث عشر الأوبئة الفضائية للمعلومات والتي أهمها الفيروسات، والقنابل المنطقية، والديدان.

أما الجزء الرابع والأخير فتناول حرب المعلومات الدفاعية، حيث تتكون من أربعة فصول تناولت أساليب حرب المعلومات الدفاعية لسد الثغرات، والانكشافات المعلوماتية، ومخابئ المعلومات، والتحقق من الأمن المعلوماتي، وحراسة المعلومات. كما تناول الفصل الرابع عشر سد الثغرات والانكشافات في البنية التحتية المعلوماتية، وخاصة التطبيقات والخدمات، وطرق البيانات بالإضافة إلى حماية القطاعات التي تشكل البناء التحتي المعلوماتي الحساس (الاتصالات، والمعلومات، والتوزيع الفيزيقي، والطاقة، والمال، والبنوك، والخدمات الإنسانية الحيوية). أما الفصل الخامس عشر فيناقش مخابئ المعلومات، وطرق حمايتها، وخاصة الحماية الفيزيقية، والتشفير، والتمويه، والإخفاء، والترشيح، والنفايات، ودرع المعلومات. ويتناول الفصل السادس عشر سلامة المعلومات، والتي تبحث في وسائل ضمان سلامة المعلومات من الناحية الفيزيقية (كالمباني، والمواقع)، والإلكترونية (الدخول إلى الحاسب). كما يتناول هذا الفصل وسائل الكشف، والضمان لسلامة المعلومات. وأخيراً يتناول الفصل السابع عشر حراسة المعلومات، ومنع وصول العابثين، والمتطفلين، والمجرمين لها، ويشمل ذلك التحكم بالدخول للمعلومات، وسياسات الدخول، والتدقيق على العاملين والعمال، ومراقبة الانكشافات، والثغرات، ومراقبة التحكم في الدخول وجدران الحماية.

لقد تناول هذا الكتاب العديد من الموضوعات، إلا أن هناك موضوعات ذات صلة لم يتم تناولها بعمق، إما لكونها فنية بحتة، أو أن المجال والوقت لا يسمحان بذلك. ولقد أنجز هذا الكتاب بفعل مساهمات الآخرين القيمة في هذا الحقل، ومن مختلف حقول المعرفة. كما أن مساهمات الكثيرين مما لا يتسع المجال لذكرهم جميعاً، وكان لها الأثر الكبير في الكثير من التعديلات، ومنهم طلاب البحث العلمي في أكاديمية نايف العربية للعلوم الأمنية، والمشاركون في الندوات، والحلقات العلمية ذات العلاقة، والشكر موصول لدورثي داينتج على موافقتها على الاقتباس من أعمالها، واستخدام نظريتها في حرب المعلومات، والشكر موصول لعبد العظيم محمد صالح

على مراجعتة وقراءته لمسودات الكتاب، ومساهمته خاصة في الجوانب الفنية، والكثير من المواقع على الإنترنت.

وأشكر عادل الربطة على المراجعة اللغوية، والأستاذ عبدربه شميت على الطباعة، والإخراج والملاحظات القيمة التي كان يبديها خلال الطباعة، وأخيراً أشكر زوجتي ريم، وأولادي تالا، ودارا، ويزن، وتمارا، ومحمد على دعمهم وحبهم، وتفهمهم لانشغالي عنهم.

ذيــاب البداينــــــــــة

dbadayneg@Yahoo.com

http:// www.badayneh0. tripod. com

الجزء الأول:

الأمن في مجتمع المعلومـات

- □ الفصل الأول: الأمن الوطني في المجتمع المعلوماتي.
- □ الفصل الثاني : الثغرات الأمنية الجديدة والتهديدات المشتركة
- □ الفصل الثالث : خصائص المجتمع المعلوماتي

تمهيد

يتناول هذا الجزء الأمن في مجتمع المعلومات. شمل هذا الجزء ثلاثة فصول هي: الفصل الأول: الأمن الوطني في المجتمع المعلوماتي وقد بحث هذا الفصل موضوعات الأمن الوطني في المجتمع المعلوماتي، وأهميته ومهدداته. في حين يتناول الفصل الثاني الثغرات الأمنية الجديدة والتهديدات المشتركة وخاصة في قطاع الاتصالات والمعلومات والتوزيع الفيزيقي، والطاقة، والمال والبنوك، والخدمات الانسانية.

واخيراً يتناول الفصل الثالث خصائص المجتمع المعلوماتي، وقد شمل هذا الفصل معايير المجتمع المعلوماتي، وخصائصه وخاصة الخصائص التقنية والاجتماعية، والثقافية والسياسية والاقتصادية والأمنية، كما يتناول الأمن العربي في عصر المعلومات

الفصل الأول

الأمن الوطني في المجتمع المعلوماتي : المفهوم والتحديات والانكشافات

مقدمة

للمعلومات دور رئيس في الأمن على مر العصور، وهذا الدور ليس وليد هذا العصر، فحياة الإنسان القديمة، وصراعه مع قوى الطبيعة منها خاصة، كان فيها الإنسان متعطشاً للمعلومة لتفسير الظواهر المخيفة بالنسبة له في تلك الأيام، وشمل بحثه عن إجابات للعديد من الظواهر حوله والتي تطلبت البحث عن المعلومات حول ماذا يحدث؟ لماذا يحدث؟ متى يحدث؟ وكيف يحدث؟ . . . إلخ. ولم يتوقف ذلك عند الظواهر الطبيعية بل شمل ذلك خوفه من الحيوانات المفترسة، والمطر، والزلازل، والكوارث . . . إلخ. وزادت أهمية المعلومات في الصراعات البشرية، وخاصة الحروب . . ماذا لدى الخصم؟ ماذا يعرف الخصم عني؟ ماذا ينوي أن يفعل؟ ماذا أفعل؟ كيف لي أن اواجه تهديداته؟ من ينتصر؟ . . إلخ. واستخدم الإنسان كافة الوسائل المتاحة لديه خدمة للحصول على المعلومة التي يمكن أن يوظفها لخدمة أمنه الفردي، والاجتماعي، والسياسي.

وعلى الرغم من كلفة المعلومات والمتمثلة في ندرتها، وقيمتها، إلا أن تقنيات المعلومات وأوعيتها قد وفرت المعلومة بمقدار كبير، وضاقت خزائن الدولة السرية ـ الموسومة بسري للغاية، أو محدود التداول ـ بما لديها، وهذه الولايات المتحدة الأمريكية تنفق حوالي (5.6) مليار دولار سنوياً على «فرض السرية» على المعلومات، ولديها حوالي (1.5) مليار صفحة حكومية عمرها أكثر من (25) سنة تحت أقفال السرية، وفي عام 1995م تم تصنيف (3.6) مليون وثيقة بأنهاسرية منها (400) ألف وثيقة وصفت بأنها سرية للغاية (مطر، 1999، ص 49). إلا أن الوثائق السرية وعلى الرغم من أهميتها، إلا أنها ليست جميعها تتصف بالموثوقية والصدق، وحالها حال الحاسب فإن المدخلات الخاطئة تؤدي إلى مخرجات خاطئة، وبالتالي فإن القرارات وخاصة الأمنية المبنية على معلومات سرية غير موثوقة ولا صادقة تؤدي إلى قرارات بالضرورة غير صحيحة ولا موثوقة، وقد تكلف الكثير. والقرار الأمني مثله مثل القرار السياسي قد تعدد فيه اللاعبون (المعنيون)، وليس الأمنيون وحدهم، بل أصبحت مراكز البحوث، ومراكز الاستطلاع العام، وشبكات الحاسب، والقنوات الفضائية والإعلام . . إلخ، كلهم مؤثرون في اتخاذ القرار وفي توجيه القرار، وفي غياب إجماعهم قد لا يحظى القرار بالقبول ولا بالتنفيذ. فالاعلام والجامعات الأمريكية دفعت بالحكومة الأمريكية إلى الانسحاب من فيتنام، وخاصة المظاهرات

الشعبية ضد الحرب في تلك الفترة، ولم تعد المعلومة بعيدة المنال كما كانت في السابق ولقد عبر عن ذلك السيناتور الأمريكي جون كيندي بقوله «لا أعتقد أن هناك أكثر من مائة صفحة، أو بضع فئات من الصفحات على الأكثر من بين آلاف الوثائق التي بحثنا فيها يكون من المهم الآن بقاؤها سراً . . .» (موثق في مطر، 1999، ص 49).

وما أدل على أهمية اللاعبين الآخرين في صنع القرار الأمني عامة من وصف الأمين العام للأمم المتحدة لشبكة إلـ(CNN) بأنها العضو السادس عشر في مجلس الأمن (مطر، 1999) دلالة على تأثيرها وعلى قوة هذا التأثير ووضعها في مصاف الدول وأحياناً أقوى منها. ولاتقل قناة الجزيرة أهمية عن ال (CNN) في تغطية الحروب والازمات . ولقد شكت الكثير من الدول وخاصة العربية من نهج قناة الجزيرة الذي لم تألفه القنوات التلفزيونية الرسمية، خاصة أن الجمهور المستهدف ليس جمهور الدولة ذات العلاقة، بل يتعداه إلى ملايين البشر في كافة أنحاء المعمورة. كما أن الدولة لاحول لها ولاقوة في منع بث القناة حيث يمكن التقاطها دون موافقة الدولة. للمعلومات قيمة عالية جداً ففي الحرب على افغانستان، حيث شكل تفرد قناة الجزيرة بالمعلومات وبث اشرطة فيديو مسجلة لابن لادن أمراً أثار غضب الادارة الامريكية، مما جعلها تصف الجزيرة بانها بوق دعاية للقاعدة وطالبان، ومما زاد الأمور تعقيداً أنه لم يستطع الأمريكان انتقاء المعلومات قبل بثها ومراقبة المعلومات وخاصة الاعلامية والسماح ببثها بعد الموافقات الأمنية كما حدث في حرب الخليج الثانية. وكذلك الحال عندما لم تعطى لعرفات فرصة بث كلمته من رام الله إلى القمة العربية في بيروت عام 2002، وقامت ببثها قناة الجزيرة مباشرة، وبالتالي اصبحت قناة الجزيرة العضو الجديد والاقوى في الجامعة العربية. والتي ليست بحاجة الى الاجماع العربي لتفيذ قراراتها.

لقد أصبحت جرائم المعلومات ونظمها، بلا حدود، وهي عالمية، والتحقيق فيها والحكم عليها عملية معقدة. وترتكب هذه الجرائم من قبل الأفراد أكثر مما ترتكب من قبل محترفي الحاسب وشبكات المعلومات. كما يمكن أن ترتكب من مراكز البحوث، ومن الأكاديميين، ومن مديرين يبحثون عن الثراء أو السلطة، أو من قبل مؤسسات تبحث عن معلومات عن منافسيها، أو من وسائل إعلام تبحث عن معلومات أو أخبار أو من قبل حكومات تبحث عن معلومات تجارية، أو جريمة منظمة تبحث عن ملفات موثوقة.

إن المعلومات مثلها مثل أي سلعة ذات قيمة مادية أو غير مادية عالية عرضة للجريمة بما في ذلك الاحتيال والسرقة والتعدي والتخريب . . .الخ. وتزداد جرائم المعلومات يومياً، وأصبحت محط حديث وسائل الإعلام والباحثين والعلماء. عندما سئل ويلي سوتن (Sutton) لماذا سطا على البنك أجاب «لأن المال موجود هناك»، والمال اليوم هو المعلومات، ولقد تعلم المجرمون اليوم مكان وجود المال، ويمكنهم من سرقة كميات كبيرة بمخاطرة أقل. ولقد تأزمت العلاقات بين الدول بسبب سرقة المعلومات (أسرار عسكرية تتعلق بتقنيات متقدمة) (وامثلة على ذلك بين الولايات المتحدة والصين، وكندا).

أدت ثورة المعلومات إلى أنماط جديدة من التحديات والجرائم منها : لصوص الحاسب الذين يدخلون إلى أنظمة الحاسب وقواعد المعلومات ويسرقونها، أو يعبثون بها، والجرائم الحديثة التي تخترق الحماية الأمنية في النظم القانونية ويتم تجنب العقاب فيها (البداينة، 1999ب). الجانب المظلم للمعلومات هو استثمارها في جوانب مهددة للأمن البشري عامة، ماذا يحدث لو لوثت مجموعة إرهابية المياه في مدينة من مدن العالم الكبرى، أو أوقفت حركة الطائرات، أو فجرت قنابل كيماوية، أو جرثومية في أي مكان. كما حدث في حادث الأنفاق في اليابان، أو كما يعتقد انه عمل إرهابي في الولايات المتحدة بخصوص الجمرة الخبيثة. والمعلومات عنصر مهم، لها قيمة، هذه الأهمية لا تتوقف عند تسيير حياة الناس، بل تتعداها إلى حمايتهم. إنها الأساس الذي تقوم عليه الحياة الاجتماعية والتفاعلات بين الأفراد، مما يجعلها عرضة للتعدي نظراً لأهميتها في تسيير أمور الخصم، ولكي يضعف الخصم وتسهل السيطرة عليه، ولذا فإن حرب البناء المعلوماتي هدف مغر وسهل التنفيذ، والمعلومات هي الأساس فيما يعرف بحرب المعلومات، حيث تستخدم المعلومات كأداة في الهجوم المعلوماتي على الخصم، وتدمير وتعطيل البناء التحتي المعلوماتي لديه، وهي إدارة دفاع معلوماتي تمنع الخصم من التعدي، وتوفير ميزات لنا في السيطرة والاتصالات والتوجيه. وللمعلومات أثر في مختلف جوانب الحياة الاجتماعية، وفي الضبط والقيادة والتحكم العسكري، هذه الآثار يمكن أن تحسم الحرب لصالح طرف على حساب الطرف الآخر، ولأن هذه الآثار مهمة في الدعم الاجتماعي للقطاع الأمني وفي التخطيط لسير العمليات والخطط الدفاعية، مما يشكل أثراً سلبياً على الطرف الذي تدمر فيه بنيته التحتيه المعلوماتيه.

كما أن المعلومات مصدر تهديد أمني نظراً لأنها تمثل رابطاً تعتمد القطاعات الاجتماعية عامة، سواء أكان ذلك في مجال الاقتصاد أم الاتصالات، هذا بالإضافة

إلى الجاذبية التي تشكلها المعلومات وخاصة الحساسة منها سواء كان ذلك في مجال التصنيع العسكري أو في المجال التجاري (التنافس بين الشركات) مما يعني الإضرار بالطرف المقابل أو الاستفادة دون عناء مما توصل إليه الطرف الآخر (عسكرياً أو اقتصادياً أو تقنياً). والمعلومات هلامية بمعنى أنها تنقل بأشكال متنوعة وتتشكل وفق الحاجة وطريقة الاستخدام وبسهولة.

تشمل حرب المعلومات قوة مضادة وقيمة مضادة، وتزداد أهمية المعلومات في الحرب بشكل كبير، وتوصيل المعلومات من خلال النظم العسكرية (القيادة، السيطرة، الاتصالات) عملية هامة تساعد على التوجيه الدقيق للضربات. أما القيمة المضادة للمعلومات فمنصب على أنها نفسها عرضة إلى الهجوم، إن تدمير البناء المعلوماتي قد يؤدي إلى هزيمة سريعة لأي دولة (جارنم، 1998).

كما أن الحصول على المعلومات قد لا يكلف الكثير من المال والجهد مما يجعل التعدي عليها (الحصول، أو التخريب، أو التشويه) عملية سهلة وغير مكلفة. ومما يزيد الأمور تعقيداً أن التعديات على المعلومات واستغلالها ضد الطرف الآخر تتم في خفاء، ويصعب فيها كشف الفاعل، أو الفاعلين، مما قد يشجع الجواسيس على إتلاف وتخريب المعلومات وعدم فضح أمرهم، أو كشف هوياتهم. كما يمكن خرق أمن المعلومات عن بعد ومن مكان بعيد جداً عن أماكنها وخاصة مع توفر الربط الكوني للمعلومات والأبنية المعلوماتية بشبكات الاتصالات. فالحدود السياسية للدولة يمكن اختراقها عن بعد من خلال الأسلحة بعيدة المدى والتخريب الإلكتروني لما بداخل الدولة وبالبث الفضائي الخارجي وبتخريب البناء التحتي المعلوماتي للمجتمع. وحيث لا ترتبط الدولة بحدود فضائية معينة، فإنه من السهل اختراق الفضاء الخارجي للدولة من خلال أقمار التجسس وشبكات الاتصال دون موافقة الدولة. ونظراً لأهمية ذلك فقد تمكنت إسرائيل من تطوير أقمارها الصناعية المخصصة للتجسس والتي أطلق أحدها في شهر (حزيران، 2002) بقصد التجسس على المجتمع العربي وباكستان ودول أخرى.

إن زيادة ترابط العالم (Connectivity)، وزيادة الاعتمادية (Dependency) بين المؤسسات المالية، والأعمال، والمنظمات، والدول، والشعوب، قد ولدت أنواعاً جديدة من المخاطر الأمنية، والتهديدات الاجتماعية (AABS, 1998)، جعلت من المستبعد أن تسفر الحرب عن فائزين، فالاعتمادية المتبادلة تقف حاجزاً دون ذلك لأن في ذلك تهديداً لمصالح الكثير من الأطراف الحكومية، وغير الحكومية. فمع زيادة

العولمة والاتصالات، واختراق الحدود السياسية للدولة تكونت بنية تحتية معلوماتية كونية جعلت مسؤولية حماية الأمن مسؤولية دولية، مما عزز عولمة وعالمية القوانين، وحماية البنى التحتية المعلوماتية الكونية. فعندما ينتشر فيروس ما على الشبكة يهدد جميع مستخدميها ومن جميع الدول.

إن الأمن متعدد الجوانب والأبعاد، ومحصناته ومهدداته الداخلية منها، والخارجية متنوعة ومتغيرة عبرالتاريخ التطوري للمجتمع الواحد، وللمجتمعات البشرية، وهي نتيجة لنمط البنى الثقافية، والاجتماعية المختلفة. ومن أكثر المهددات أهمية في الأمن هو ما يصيب المجتمع من تغيرات مفاجئة، وتحولات سريعة في البنى الاجتماعية والاقتصادية للمجتمع (مجتمع زراعي ـــــ صناعي ـــــ معلوماتي)، خاصة أن المجتمع المعلوماتي قد أحدث تغيرات كبيرة في فترة زمنية وجيزة، فاقت الكثير من تراكم التغيرات عبر عشرات السنين وكذلك فإن المشكلات الاجتماعية العامة كالبطالة، والفقر، والأمية والتي تفاقمت بفعل هذه التغيرات قد شكلت مهددات لأمن الفرد، والمجتمع. كل هذا أدى إلى أن أمن المجتمع المعلوماتي ما هو إلا نتيجة وظيفية لنوعية البنى الاجتماعية، والاقتصادية للمجتمع المعلوماتي.

الأمن ضرورة اجتماعية، لابد من توافره واستتبابه ليتمكن الفرد والمجتمع من أداء الوظائف الاجتماعية المناطة بهما. وجوانب الأمن الاجتماعي الرئيسة متمثلة بأمن الجسد، وأمن المعتقد، وأمن النفس، والنسل، والمال، والعقل. وإن حفظ الأمن في هذه الجوانب يؤدي إلى الاستقرار الاجتماعي العام. ويمكن التنبؤ بالأمن في أي مجتمع من عدة مؤشرات أهمها الرخاء الاقتصادي الذي يعد نصيب الفرد من إجمالي الناتج القومي (GNP Per capita) مؤشراً عليه، وكذلك من خلال الاستقلال الاقتصادي، والاكتفاء الاقتصادي الذاتي، وفي المجتمع المعلوماتي وفي عصر العولمة، فإن الاقتصاد العالمي مترابط وحساس للتغيرات التي قد تحصل في أي موقع اقتصادي هام (مثل الاقتصاد الأمريكي، أو الياباني)، لما يجعل الأمن الدولي وليس وطني فقط.

ونظراً لأهمية الأمن في التنمية الاجتماعية والاستقرار العام للمجتمع فقد تخلى المواطن الاميركي عن حريته أو جزء كبير منها لصالح الأمن، وذلك من خلال السماح للـ FB1 بالتجسس عليه لمكافحة الارهاب وصده.

فالأمن مطلب أساسي لكافة النشاطات الإنسانية على مستوى الفرد وعلى مستوى المجتمع. والقطاع الأمني القومي هو القادر على تحقيق البيئة المناسبة للتنمية الشاملة،

ولقد أكد تقرير وزارة الدفاع البريطانية في المؤتمر الدولي عن التطور الدولي والمنعقد خلال الفترة 15-2000/2/17م، بعنوان «إصلاح القطاع الأمني وإدارة النفقات العسكرية: مخاطرة كبيرة للمتبرعين، عائدات كبيرة للتنمية»، يذكر فيه :

«تحتاج الدول النامية أن تكون قوى أمنها فاعلة وفعالة وخالية من الفساد، إنهم الفقراء الذين يدفعون الثمن إذ وضعت الدولة كامل مقدراتها في الجيش وتركت القليل للصحة والتعليم. وتحتاج الدول النامية أن يكون قطاعها الأمني تحت السيطرة المدنية لأن الفقراء سيعانون كثيراً على المدى البعيد من فشل تحقيق المسؤولية» .(DFID, 2000, p. 4)

وأكد التقرير على جودة القطاع الأمني اللازمة لتحقيق الأمن فذكر :

«أن القطاع الأمني المسؤول والمدرب جيداً، ومحكم البناء يمكن أن يقدم ويساعد في تقديم بيئة آمنة وحامية للفقراء والمجتمعات المحلية. ولكن العكس عندما يكون القطاع الأمني غير متماسك، وضعيف الإعداد، وقمعياً فإنه يمكن أن يكون مصدراً رئيسياً من اللا أمن ـ بفعل العنف ذاته بدلاً من حماية الناس من العنف» .(DFID, 2000, p. 7)

لقد شكلت السيادة الوطنية عنصراً مهماً من مصادر الصراع بين الدول، وخاصة في مجال الحدود والتدخل في الشؤون الداخلية، فبالإضافة لما تحمله السيادة الوطنية من معاني الهوية والانتماء، و الوجود، والاستقلال، فهي تحمل معاني تتعلق بمكانة الدولة والمجتمع، والهيبة المحلية والدولية لهما، وتحمل جوهر وجود الدولة واستقلاليتها. غير أن السيادة الوطنية قد تميعت في المجتمع المعلوماتي، وما عادت تستمد شرعيتها من الانتخابات ولا المجالس الوطنية الشعبية والحكومية. فالحدود لم تعد كما كانت تمنع وتنتقي الداخل والخارج منها، ولم تعد تعمل كمصفاة للداخلين والخارجين، المرغوبين والمطلوبين للدولة أو بين الأصدقاء والأعداء. فهذه الجماعات الأهلية العابرة للحدود مثل أطباء بلا حدود، وجماعة السلام الأخضر وغيرها، تعمل على مستوى العالم، وهذا مفهوم المواطنة الكونية يحل محل المواطنة المحلية. فنجد أن جماعة مثل جماعة السلام الأخضر قد أثارت في فرنسا قضايا المخلفات النووية ودفنها في البحار، جماعة تتغلب على دولة وتجعلها تتراجع عن قرارها. وهذه جماعات حقوق الإنسان تجبر الدول على فتح سجونها ومعتقلاتها للتحقيق، وتشترط معونات اقتصادية، وأحياناً تعلق عضويتها في المجالس الدولية الهامة بسجل حقوق

الإنسان فيها، وهذه الصحافة تحرج الحكومة البريطانية بتصريحات ومقابلات «مفخخة» مع زوجة أحد أبناء ملكة بريطانيا، وهذه الولايات المتحدة تبتعد آلاف الاميال عن حدودها الوطنية لتتجسس على الصين، والشرق الأوسط، وإيران، والهند، والباكستان . . . إلخ. وما حادثة طائرة التجسس الأمريكية التي هبطت مضطرة في الصين (نيسان، 2001م)، إلا مثالاً من العديد من الأمثلة. وهذا صندوق النقد الدولي يملي شروطه على الدول وتخافة الدول أكثر مما تخاف لجان المراقبة والتشريع في مجالس نوابها، أو أي مؤسسة تشريعية، أو رقابية أخرى. وها هو أحد أفراد الوفود الأمريكية في عصبة دافوس وبلا جيش، ولا راية، ولا أرض، ولا جنسية يتهم رئيس وزراء منتخب بشرعية شعبية ومرجعية قانونية ودستورية ويقول لرئيس وزراء ماليزيا إنه يشكل خطورة على مصالح ماليزيا (مطر، 1999).

وتهدد المعلومات الأمن الوطني، ذلك أن البناء التحتي الاجتماعي والاقتصادي والعسكري والاتصالات مبني عليها، ونظراً لأن المعلومات مكشوفة فإن ذلك يسهل مهاجمتها. فوضع فيروس في شبكة الحاسب الوطنية قد يؤدي إلى شل حركة المجتمع الاقتصادية أو الاجتماعية (التواصل بين الأفراد). إن أي تعد على أي موقع من مواقع البناء التحتي المعلوماتي من شأنه أن يجعل المجتمع والدولة لا ترى ولا تسمع ولا تتكلم وتسهل السيطرة عليهما.

وحتى الاقتصاد لم تعد الدولة تسيطر عليه، فقد عبرت الشركات الكبرى الحدود الوطنية وتعددت جنسياتها، وتملك من الثروة والمال مالاتملكه العديد من الدول. فهناك أكثر من (100) دولة أقل ثراء من أي من (40) شركة عملاقة، وهناك (200) شركة متعددة الجنسيات تنفذ حوالي ربع النشاط الاقتصادي الدولي، وتستخدم (0.057) من القوى العاملة الدولية.

في هذا العصر ازدادت فكرة فصل الأرض عن الدولة اتساعاً وقبولاً وتمثلت فيما يطلق عليه المناطق الحرة، والمستخدمة لغايات التجارة والعبور، وهي مناطق «بلا سيادة وطنية» وبعضها في حالة «إيقاف السيادة» لفترة معيّنة. ولم يتوقف الفصل بين الأرض والدولة، وإنما تعداه للمواطن فالمواطن يعيش في بلد وهو في واقع الأمر ينتمي إلى بلد أكثر من حدوده الوطنية فهو يلبس من بلد ويتغذى من بلد آخر، ويتكلم بلغة غير لغة البلد، أو المجتمع، ويتواصل مع المجتمعات الأخرى، يتحاور مع زملاء وأصدقاء خارج حدود الوطن هو هنا في الوطن وهو هناك في العالم التخيلي. وتمثل هذا في عولمة الثقافة والأمن والحرية، والقانون، وكل شيء. هذا الانفصال بين المواطن

والأرض لم يتوقف عند هذا الحد بل تعداه إلى الانفصال بين المواطن والمواطن، فهذه الأقليات تنزع إلى الاستقلال والتمرد، والمطالبة بحق تقرير المصير، وهذا مثال يضربه مطر على النزعة الاستقلالية، أو الانفصامية بين المجتمع الواحد، فجورجيا التي استقلت عن الاتحاد السوفياتي، ما لبثت الأقلية الأبخازية فيها تطالب باستقلالها وحق تقرير المصير، ومع المساعدات الروسية لجورجيا في وقف هذا الانفصال، أو الاستقلال، إلا أنه من الممكن بعد حصول الأبخاز على حق تقرير المصير، أو الاستقلال أن يطالب أبخاز الشمال (المسلمون) بالانفصال عن ابخاز الجنوب (المسيحيون) (مطر، 1999).

إن التوازن العادل بين دعم محصنات الأمن والتنمية البشرية أمر هام، إن تمتع الدول بالسيادة يعني الاستقلالية في اتخاذ القرارات، إلا أن ذلك قد يؤدي إلى فوضى دولية حيث أن الدولة تعمد إلى التسلح والإنفاق عليه للمحافظة على مستوى عال من القوة لردع أي تهديد خارجي ودحره، وبالتالي فإن الموازنة بين المدفع ورغيف الخبز عملية في غاية الأهمية.

الأمن : المفهوم

الأمن الوطني كما يعرفه بترسون(Peterson) «الإدراك الجمعي للإحساس بالأمن» (موثق في Devost,1995, p. 19)، ويعرف ولتمان وناشت، وكويستر الأمن بأنه «مجموعة من التهديدات الفيزيقية (Physical) والتي ربما تواجه الدولة، وتدفع بالبنى والعقائد، والسياسات العسكرية للتأهب لمواجهة هذه التهديدات. . .وهذه عوامل داخلية وخارجية، مثل التغيرات الاقتصادية والاجتماعية التي ربما تؤثر بطريقة مباشرة أو غير مباشرة، وتنقص أو تزيد من قدرة الدولة على مواجهة التهديدات الفيزيقية (موثق .(Devost, 1995, p. 19

في حين يستند الأمن الجماعي إلى قيام أعضاء في مجموعة محددة من الدول بنبذ استخدام القوة فيما بينها، والتعهد بالدفاع المشترك عن أي عضو في المجموعة يتعرض لتهديد، أو هجوم من أي طرف خارجي. أما الأمن الشامل فيركز على التعاون وبناء الثقة والمكاشفة، ونزع السلاح، في حين يتناول الأمن الشامل جميع الاحتياجات الإنسانية المهددة للبقاء على مستوى الفرد، والجماعة، والدولة، والاقليم، والكون . اما الأمن الانساني فيركز على الكرامة الإنسانية، ويشمل حماية الإنسان من تهديدات الجوع، والمرض، والقهر كإنسان. ولقد ساهم انتشار شبكات المعلومات في تكوين جماعات ضغط دولية تتواصل عبر الإنترنت، وأصبحت عابرة

للحدود الوطنية، لا بل أصبحت حدودها العالم بأسره. فانتشار الجماعات والمنظمات غير الحكومية قد شكلت أبنية جديدة في مجالات عديدة (حماية البيئة، والصحة، والعدالة الاجتماعية وحقوق الإنسان . . . إلخ.).

أما الأمن الدولي فلا يتوقف على استتباب الأمن بين الدول من الناحية السياسية، بل أصبحت مسؤولية المحافظة على الكوكب أمناً، مسؤولية دولية، حيث إن مهددات البقاء للعالم لا تميز بين دولة غنية ودولة فقيرة، أو نامية ومتقدمة، فمشكلة الأوزون والتلوث، وأسلحة الدمار الشامل، وتهديد الثروة النباتية، والحيوانية، والأسماك . . . إلخ، كلها مهددات تنال من البشرية جمعاء، ومن الكوكب الذي يمثل بيت البشر أجمعين (البداينة، 2005 أ، ب).

ويذكر تقرير لجنة إدارة شؤون المجتمع العالمي (1995) عدداً من المبادئ لإقامة الأمن في عالم الغد منها :

1- حق كافة الناس بالوجود الآمن، وضرورة التزام الدول بحماية هذا الحق.
2- ضرورة منع الصراع والحروب كأهداف أساسية للأمن العالمي، وتعزيز ظروف الحياة، والنظم المعززة لها وإزالة الظروف الاقتصادية، والاجتماعية، والبيئية، والسياسية، والعسكرية المهددة لها.
3- استباق الأزمات وإدارتها قبل تصاعدها إلى صراعات مسلحة.
4- عدم استخدام القوة العسكرية كأداة سياسة مشروعة إلا بالدفاع عن النفس.
5- عدم تنمية القدرات العسكرية أكثر من الحاجة الوطنية، حيث يعد ذلك تهديداً للأمن العالمي.
6- أسلحة الدمار الشامل أدوات مشروعة للدفاع الوطني (لجنة إدارة شؤون المجتمع العالمي، 1995، ص 104).

الأمن من المنظور المعلوماتي

المعلومات ثروة، وهي بناء تحتي ترتكز عليه النظم السياسية والاجتماعية والتربوية والإدارية الحالية. وهي ذات قيمة عالية وثمينة مما يجعلها عرضة للتهديد والتعدي والخرق من قبل العابثين والمتلصصين وقراصنة الحاسب والمجرمين. وهي مصدر مهم من مصادر الثروة في المجتمعات واكتسابها يتطلب مهارات عالية، وقيمتها لم تختف على مر العصور وبخاصة في مجالات التجسس والخدع العسكرية. . . الخ، حيث شكلت كلها وسائل بحث عن المعلومات عن الذات وعن الآخر.

في مجتمعات اليوم يحتدم الصراع حول عناصر الثروة، والقوة، والمكانة، وهي ذات العناصر التي يتنافس عليها الفرد. وتولد هذه العناصر صراعاً بين الدول نظراً لمحدوديتها، وندرتها. و هناك كميات هائلة من الثروة المجتمعية يتم تطويرها، أو تخزينها، أو نقلها، أو انتقاؤها باستخدام وسائل نقل المعلومات وتخزينها كالحاسب، فالقطاع الخاص في كثير من الدول يحول مليارات الدولارات من العمليات المالية يومياً من خلال الشبكات الإلكترونية المحلية والدولية (البداينة، 1999 أ، 1995 أ ب).

ولدت المعلومات أنموذجاً جديداً في الأمن (New Paradigm)، لقد كان الصراع بين الدول ولا يزال يتعلق بالعناصر الأساسية للثروة، والقوة، والمال، والمكانة. ولقد تطورت مستلزمات هذه العناصر من السلاح والصناعة العسكرية والمصادر الأساسية للطاقة والأسواق مما أدى إلى استعمار دول لأخرى وسيطرة بعض الدول بطريقة مباشرة أو غير مباشرة على أخرى، ومكانة الدولة وهيبتها عامل أساسي تحصل عليه الدول من مميزات دولية سياسية، أو اقتصادية . . . إلخ، وتحدد الأدوار التي يمكن لدولة ما أن تلعبها، وفي المجتمع المعلوماتي شكلت المعلومات البنية التحتية للمجموعات ولمؤسساتها، ومع زيادة الاعتماد على تقنيات المعلومات زادت احتمالية التعرض للفشل أو التخريب مما يهدد الأمن الوطني للمجتمع والدولة.

يمكن تعريف الأمن الوطني من المنظور المعلوماتي على أنه «الاحساس الجمعي الفعلي والتخيلي بعدم وجود و/أو تأثير التهديدات الفيزيقية والتخيلية لبنى المجتمع المعلوماتية (وخاصة الحساسة منها) في جوانبها العسكرية، والاجتماعية، والثقافية، والاقتصادية . . . إلخ.) المختلفة أياً كان مصدرها داخلي (مشكلات اجتماعية)، أو خارجي (صراعات، وحروب)، وتستدعي التأهب و/أو الفعل الاجتماعي و/أو التأهب والفعل الرسمي لمواجهتها. ويشمل هذا التعريف على العناصرالتالية :

1- الاحساس الجمعي الفعلي والتخيلي، ويشمل الاحساس الرسمي و/أو الاجتماع لمؤسسات المجتمع بوجود خطر / تهديد، قديكون هذا التهديد موجوداً فعلياً أو تخيلياً (شيوع مخاوف بتهديد ما)، وقد يكون هذا الاحساس مبرر اً منطقياً وواقعياً، وقد لا يكون.

2- التأثير : قد يتواجد التهديد ولكن دون تأثير فوجود التهديد لوحده غير كاف إن لم يكن على درجة من التأثير كافية لاثارة الاحساس الجمعي بتهديد الأمن.

تحديات المجتمع المعلوماتي

أدت ثورة المعلومات إلى ظهور أنماط جديدة من التحديات الأمنية. ولقد ظهرت تحديات جديدة للأمن بمفهومه التقليدي، هذه التحديات تتعلق بالاستعدادات اللازمة للتعامل مع المستجدات والمهددات الأمنية. ففي السابق يمكن للدولة إغلاق حدودها والتشويش على جيرانها وعدم استقبال بثهم التلفزيوني، ومنع الاتصالات معهم. وكانت غالبية المهددات الخارجية تأتي من الجيران لخلافات حدودية، أو أطماع في المصادر الوطنية، أو بسبب تحالفات عسكرية معينة. أما في المجتمع المعلوماتي فلم يعد بالضرورة أن تكون الدول متجاورة لكي تهدد بعضها أمنياً، فتطور نظم السلاح الذي مكنه من الوصول لمسافات بعيدة، واستخدام تقنيات بسيطة لتدمير البناء المعلوماتي للدولة وتخريب نظمها الإدارية، والعسكرية، قد جعل حرب المعلومات حرب الجميع، وان جيشها الجميع صغاراً وكباراً، هواة أو قراصنة ومتلصصين،أفراداً وجماعات. . . . . . الخ (البداينة، 1999ب).

ويمكن القول إن الأمن في المجتمع المعلوماتي ما هو إلا نتيجة طبيعية لتطور بنى المجتمع وانتقالها من مجتمع صناعي إلى مجتمع معلوماتي. وانتقل أساس القوة من الارض (المجتمع الزراعي) إلى الآلة (في المجتمع الصناعي) إلى المعلومات (في المجتمع المعلوماتي) إلا أنه يمكن القول إن سرعة انتقال التقنيات بين الدول، وتوافر البنية التحتية المعلوماتية الأساسية قد سرع في انتقال المجتمعات النامية إلى المجتمع المعلوماتي على الرغم من أنها غير منتجة تقنياً لهذه المعدات، ومتخلفة معلوماتياً. أصبحت المشاركة الدولية في كل شيء، في الحدود، والاقتصاد، والفضاء، والثقافة، الطعام، وفي التهديدات الأمنية كذلك (البداينة، 1999 ج).

هناك مجموعة من التحديات التي نجمت عن المجتمع المعلوماتي منها التحديات على المستوى العالمي، والتحديات على المستوى الوطني، وذلك على النحوالتالي :

أ ـ التحديات العالمية، وتشمل على التالي :

1- التحديات السياسية : إن الحاجة للمعلومة حاجة قوية، والقوة هذه ذات تأثير في القرار السياسي في أي مجتمع. فمن يملك المعلومة يملك القوة التي تؤثر على صانع القرار السياسي في أي مجتمع إن كان بحاجة إلى تلك المعلومة.

2- التحديات الاقتصادية : إن نقص الموارد الاقتصادية يعني الحاجة إلى المعلومات التي تطور اقتصاديات الدول، وحاجاتها المستقبلية، فتطوير صناعة الأسماك،

والزراعة . . . إلخ . ، كل هذه التقنيات ذات تأثير في القطاع الاقتصادي للدولة.

3-التحديات التقنية (التكنولوجيا) : هناك تحد تقني يتمثل بحاجة الدول والمجتمعات إلى المعدات والبرمجيات، وإلى تطوير إمكانياتها الذاتية في هذا المجال، وهذا التطوير بحاجة إلى المساعدة الفنية والاقتصادية الخارجية.

4- التحدي الأمني: ويتمثل في ضعف البناء التحتي المعلوماتي الكوني وانكشافه للتعديات ووجود ثغرات أمنية كبيرة، إن تعطيل هذا البناء أو تخريبه أو التعدي عليه يؤدي الى اضطراب كبير في عمليات التواصل في مجالات المال والاعمال والعلاقات الاجتماعية بين الافراد . . .الخ. كما أن زيادة احتمالات وسهولة شن عمليات ارهابية معلوماتية لازالت قائمة وكبيره. بدأ الميل نحو مفهوم دولي للأمن وذلك لأن العالم يشترك في البناء الفضائي العام (وهو مشاع) وفي البنية المعلوماتية التحتية (مثل الإنترنت)، مما جعل مهددات الأمن عالمية وتتطلب حلولاً عالمية، فمثلاً إن نشر فيروس معين يهدد كل المستخدمين في كل الدول، ومن الممكن أن يخرب النظم والمعلومات في أي دولة. وازدادت الشراكة الدولية في الأمن مما يستدعي مزيداً من العولمة للقوانين، فبعد أن كان التركيز على البعد الوطني أصبح التركيز على البعد الدولي. وكذلك الحال نلاحظ الميل الدولي إلى حل النزاعات بشكل دولي والابتعاد عن الحلول الثنائية، أو المنفردة، هناك إدراك دولي للمسؤولية الأمنية وخاصة في مجالات مثل الإرهاب والمخدرات، وحتى الحروب أصبحت تأخذ الصبغة الدولية، وتحاول إضفاء شرعية دولية عليها، ويلاحظ تفعيل محكمة العدل الدولية ومحاكمة مجرمي الحرب. لقد نشطت الحركات الاجتماعية على المستوى الدولي مثل جماعات حقوق الإنسان وبدأت المنظمات غير الحكومية الدولية تمارس دوراً ضاغطاً في مجالات متعددة منها حقوق الإنسان.

ب ـ التحديات الداخلية، وتشمل التحديات التالية :

1- تحدي التنمية والديموقراطية وحقوق الانسان ويشمل: تحدي التخلف وضغوطات النمو التي تقع على كاهل المجتمع، فالفقر والأمية، والجريمة، والمشكلات الاجتماعية المتنوعة، والفساد الإداري والسياسي تحد من فرص

التطور والانتقال إلى المجتمع المعلوماتي، فلا بد من تطور البنى الاجتماعية والاقتصادية حتى تتمكن المجتمعات من دخول المجتمع المعلوماتي بيسر.

2- التحدي البشري ونقص الكفاءات : إن نقص الكفاءات على مستوى القيادة والتقنية بسبب عدم التأهيل وهجرة العقول جعل أمر التعامل مع العصر القادم في ظل مشكلات متعددة داخلية يشكل تحدياً كبيراً.

3- التحدي الثقافي : إن السير ومواكبة المجتمع المعلوماتي لابد من أن يتماشى ذلك ثقافياً مع مركبات وبنى المجتمع المعلوماتي، فلا تستطيع دولة أن تصل إلى مستوى متقدم من البنى الاقتصادية والتقنية، دون تأقلم ثقافي وتكوين ثقافي معلوماتي.

4- التحديات التربوية : يمثل النظام التربوي أكبر تحد في نقل المجتمعات إلى المجتمع المعلوماتي، فنظام التعليم لا بد أن يبنى على أسس المعلوماتية وتحويله من الاعتماد على النظم التقليدية الى تكوين بناء معلوماتي تحتي متكامل يشمل ذلك مهارات التدريس والمنهاج.

5- التحدي الأمني : يشكل الأمن اساسي التنمية المستديمة. أن عمليات التحول الاجتماعي من صيغة اجتماعية تتطلب تغيراً اجتماعياً، يؤدى الى عدم الاستقرار في البنى الاجتماعية. أن التحول للمجتمع المعلوماتي يتطلب استقرارا أمنياً قبل وأثناء عمليات التحول الاجتماعي لمجتمع المعلومات.

ويحدد بورشجريف وآخرون (Borchgrave et. al, 2000) المهددات المستقبلية الفضائية (Cyber threats) التالية :

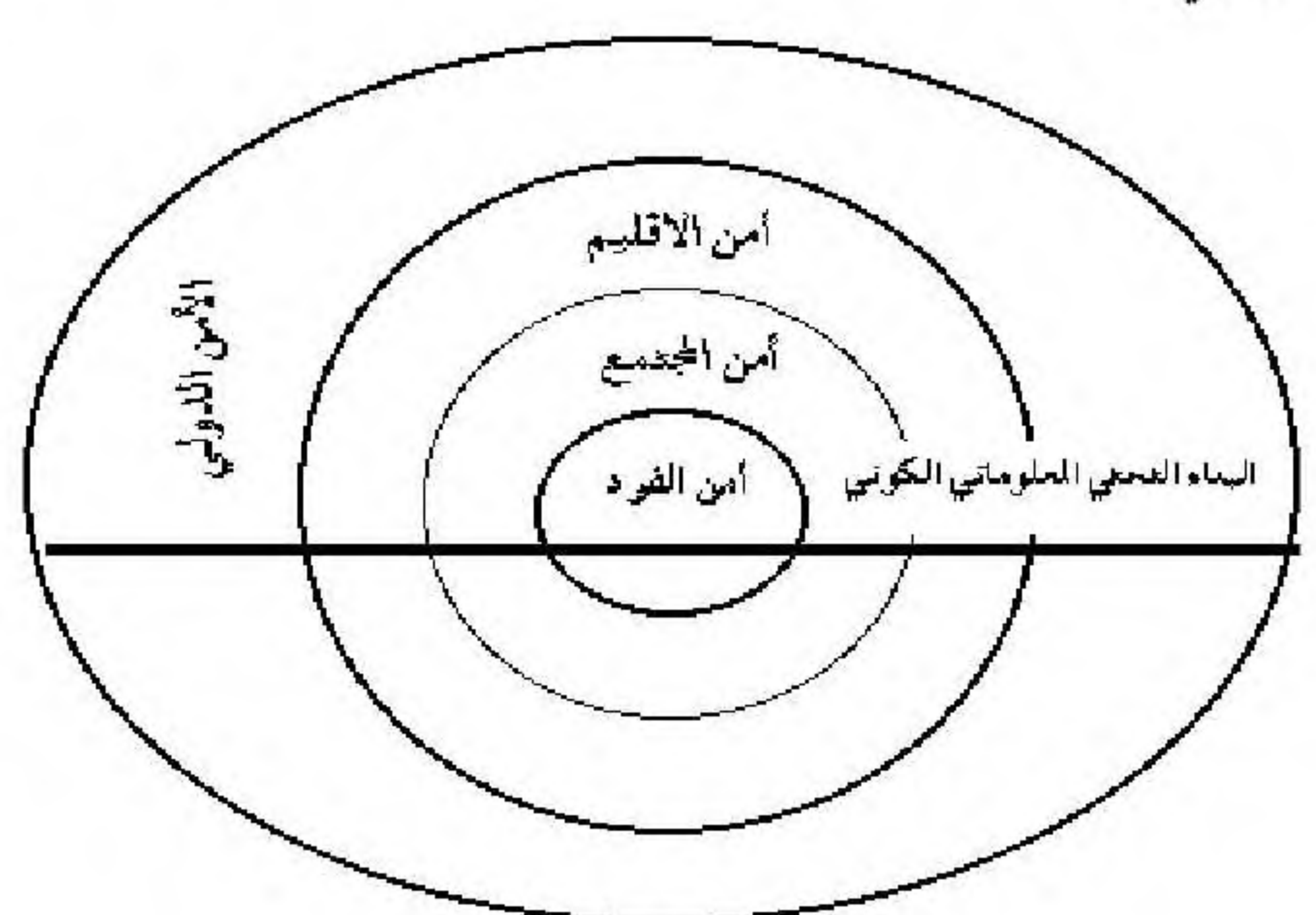
1- التهديد بالاضطراب في تدفق الاتصالات، والتحويلات المالية، والحملات المعلوماتية الهامة، ومحطات الطاقة، والمناقصات السياسية، والاضطرابات في زمن الحرب قد يؤدي إلى الهزيمة والخسارة.

2- التهديد باستغلال المعلومات الحساسة، والملكية، والمعلومات السرية. إن سرقة المعلومات أو الاحتيال بها، أو الجرائم الفضائية لها آثار سلبية على المستوى الفردي (سرقة الهوية)، وعلى المستوى المؤسسي (سرقة بطاقات الائتمان)، وعلى المستوى الوطني (المعلومات السرية).

3- التهديد بانتقاء المعلومات لاغراض سياسية، أو اقتصادية، أو عسكرية، واستغلالها أو تدميرها.

4- التهديد بتدمير المعلومات، أو تدمير مكونات البناء المعلوماتي التحتي الحساس، ولهذا نتائج سلبية كبيرة على الاقتصاد والأمن الوطني (مثل الفيروسات).

ويمكن القول إن التحديات الأمنية الجديدة إنما هي تطور لسلوكيات الإنسان في ظل البنى الاجتماعية التحتية لمجتمع المعلومات، فالمسميات الجديدة مثل السرقة الإلكترونية (Cyber)، والتجسس، والإرهاب الإلكتروني أو الفضائي (Denning, 2000) ما هي إلا أمثلة للجريمة بثوبها المعلوماتي. لقد كونت المعلومات بيئة جديدة للجريمة، فبقيت أسباب الجريمة ذاتها (شخصية، مؤسسية... إلخ)، ولكنها أصبحت تعمل في بيئات عالمية لا مسؤولة. ويظهر الشكل (1) مستويات الأمن المختلفة (الفردي ـ الدولي).



شكل رقم (1)
مستويات الأمـن في المجتمع المعلوماتي

إن الأمن الدولي من المنظور المعلوماتي يعني حماية البنية المعلوماتية الكونية من كافة التهديدات الراهنة والمحتملة، وهذا يستدعي شراكة كونية في العديد من القضايا، والمواضيع التي تهدد الأمن الكوني. ومع هذه التطورات في مفهوم الأمن وتغيره من الأمن الوطني إلى الأمن الدولي، فقد ظهرت معانٍ جديدة للأمن العالمي منها الأمن

المشترك والأمن الجماعي، والأمن الشامل. ولقد استخدمت لجنة قضايا نزع السلاح والأمن برئاسة أولف بالم مفهوم الأمن المشترك حيث أن الأمن الدائم لن يتحقق حتى يصبح أمناً مشتركاً يتقاسمه الجميع، ويشارك به الجميع، وأنه لا يمكن تحقيقه إلا بالتعاون المبني على الإنصاف، والعدل، والتبادلية (لجنة إدارة شؤون المجتمع العالمي، 1995).

وتتسائل دورثي داينج هل الارهاب الفضائي قادم؟ في اشارة الى ما بعد احداث 9/11، حيث بدأ قراصنة الحاسب والدخلاء والمقتحمون بتحويل الانترنت الى ساحة معركة. فقد اعلنت مجموعة تسمى نفسها المنذرين (Dispatchers) انها ستدمر خادمات العرب والانترنت في افغنستان والدول التي تدعم الارهاب.

وقد قامت المجموعة التي يقودها موظف أمني (21) سنة من العمر من اوهايو بمحو مئات المواقع منها السفارة الايرانية، والمواقع الفلسطينية، وهناك مجموعة أخرى تسمى نفسها القراصنة الشبان الاذكياء ضد الارهاب (YIHAT) ادعت اختراقها لبنوك اسلامية تدعم اسامة بن لادن.

وهناك مجموعة اسلامية هاجمت جماعة الشبان الأذكياء ضد الارهاب (YIHAT) وقالت أنها تدعم اسامة بن لادن. وهناك جماعة تسمى نفسها «انصار بن لادن على الشبكة» هددت بمحو المواقع العسكرية الامريكية والانجليزية، وارسلت رسائل مع صور للاطفال القتلى من الفلسطينيين على ايدي الاسرائيلين (Denning, 2001 a) .

وإذا كان الارهاب الفضائي قادم، فإن الارهاب عبر الانترنت قد أصبح حقيقة ويمثل هاجساً أمنياً، ليس على المستوى المحلي فحسب بل على المستوى الدولي كذلك، حيث اصبحت الانترنت ملاذاً أمناً للجماعات الارهابية، وعصابات الجريمة المنظمة، والجواسيس . . . الخ (راثمل، 1998). ولقد اصبحت الجريمة الالكترونية شائعة وتنفذ بأمان من المجرمين وعن بعد. في عام 1999م وقعت حوالي (2) مليون حادثة احتيال بواسطة بطاقات الائتمان عبر الشبكة في أوروبا، وزادت القرصنة والابتزاز، والتزييف، والاحتيال (فليسون، 2000).

الفصل الثاني

الثغرات الأمنية الجديدة والتهديدات المشتركة

مقدمة

تشكل البنية التحتية المعلوماتية هدفاً جذاباً لعمليات حرب المعلومات الهجومية، ففشل هذه البنية في أداء وظائفها يؤدي إلى اغراق المجتمع مباشرة بتعتيم معلوماتي وحرمان من الخدمة وفقدان التواصل مع الآخرين، وخلق فوضى اجتماعية كبيرة.

وإذا تخيلت أنك في مدينة بلا كهرباء ولا هاتف، ستتعطل لديك الاتصالات مع الآخرين، ويتعثر إنجاز عملك، ولا تستطيع سحب أي مبلغ من حسابك البنكي ولا تستطيع السفر ولا الحركة من مكان لآخر. بالاختصار تصبح أسيراً، أو مقيماً إقامة جبرية في منزلك دون خدمات، وقد تتدهور صحتك بسبب عدم القدرة على تشغيل ثلاجتك و مصفاة المياة في منزلك بسبب انقطاع الكهرباء.

يعاني البناء التحتي المعلوماتي من ثغرات أمنية، وانكشافات للعمليات العدوانية فالبنوك والمؤسسات المالية والتلفونات ومحطات الطاقة والمطارات والخدمات الحكومية الأساسية كالماء والطوارئ من أكثر المواقع حساسية عند تعرضها لأعمال المتطفلين أو الدخلاء أو المجرمين، ولقد زاد الاهتمام باستهداف البنية التحتية المعلوماتية الوطنية (NII) مع بداية التسعينيات ،ومع زيادة الاعتمادية المجتمعية والحكومية على المعلومات، مما دفع إلى تكوين بناء تحتي معلوماتي وطني للدولة. وتشمل التهديدات تخريب وتدمير المنظمات والمؤسسات والشركات والأفراد في قطاع المعلومات عامة، وخاصة الحاسبات والبرمجيات والاتصالات الفضائية ونظم الاتصالات المتصلة بالبنية التحتية المعلوماتية. أما النشاطات العدوانية فتشمل : الحرمان من الخدمة أو تعطيلها أو استغلالها للمعلومات ونظم التشغيل وخدمات الاتصالات والمراقبة غير المصرح بها للحاسبات، ونظم الاتصالات وقطاع المعلومات، والتعديل غير القانوني أو التدمير لرموز الحاسب وبرامجه وللشبكات وتحوير المعلومات، والخدمات المتعلقة بالحاسب أو الاقمار الصناعية مما يؤدي إلى خسارة كبيرة.

وتتفاقم المشكلة عند الثغرات الأمنية في البناء التحتي المعلوماتي الكوني، حيث لم تعد البنية التحتية المعلوماتية الوطنية هي الهدف، بل الكونية كذلك، خاصة مع زيادة الاعتمادية الدولية على هذه البنية في الاتصالات، والتجارة، والمواصلات . . . إلخ.

لقد أصبح تهديد أمن البنية التحتية المعلوماتية عابرةً للحدود الوطنية، فهذه الولايات المتحدة تختار اثنين من العلماء البلجيكيين لتقديم التشفير اللازم لحماية أسرار الحكومة الأمريكية، ويعبر عن هذه المخاوف مدير مركز حماية البناء التحتي الوطني في الـ (FBI) فيتس (Michael Vatis) بقوله :

«نحن بحاجة إلى الاستعداد للجهات الإرهابية الخطرة على نظم البناء التحتي الحساس، وإن أدوات العدوان (الجريمة الفضائية) معقدة ومتوافرة لأي شخص يمكنه الوصول للإنترنت» (Girard, 1998, P. iii).

ولا يتوقف الأمر على الثغرات في البنية التحتية المعلوماتية الوطنية، بل يمكن مهاجمة النظم المعلوماتية الكونية والهدف من ذلك :

1- سرقة المعلومات (Theft of Information) سرقة معلومات خطط العدو، والاستراتيجيات الاقتصادية . . . إلخ.
2- تعديل المعلومات (Modefication of Information) تغيير المعلومات وزرع معلومات خاطئة أو فيروسات.
3- تدميرالمعلومات (Destruction of Information)، مسح المعلومات التي تشمل على معلومات مالية، أو عسكرية، أو حكومية.
4- تدمير معلومات البنية التحتية المعلوماتية (Destruction of the Information Infrastructure) من خلال الفيروسات (موثق في Gumahad 11, 1996)، (موثق في Schwartau, 1982).

فمثلما شكلت الصواريخ العابرة للقارات نوعاً جديداً من التهديدات الأمنية بين الدول، فإن تكنولوجيا عصر المعلومات قد قدمت تحدياً جديداً للأمن الوطني، حيث نهاية الجغرافيا وغياب المسافات. وإن الهجمات على نظم المعلومات حقيقة واقعية في عصر المعلومات ولا زالت هذه الهجمات قليلة الخسائر، ولكنها مرشحة للزيادة ولقد قدر بأن أكثر من (90%) من هذه الهجمات قد نفذت باستخدام المعدات المتوافرة والوسائل المتاحة والتي يمكن لاي شخص استخدامها (تقرير CERT). وفيما يلي مجموعة من الامثلة:

شنت جبهة تحرير الإنترنت عام 1994م هجموم على شركة ان بي سي (NBC)، وحول المحتالون الروس حوالي (10) مليون دولار من ستي بنك (Citi Bank) إلى حسابات مستقلة في العالم. وقام روبرت موريس (Morris) ـ ابن أحد الخبراء الرواد

الحكوميين في أمن الحاسب في مركز الحاسب الوطني (NCC) وهو فرع من وكالة الأمن القومي (NSA)، وهوطالب دراسات عليا في جامعة كورنيل ـ بزرع فيروس أدى إلى خراب وخسارة كبيرين، واتهم بسوء استخدم الحاسب والاحتيال والحرمان من الخدمة (DOS).

انتقم بورليسون (Burleson) بإدخال برنامجٍ في شركة بيت السمسرة في تكساس تسبب في حذف (168) ألف سجل عمولات بعد فصله بثلاثة أيام من الشركة. وقام ألفي إخوان (The Brothers Alvi) بوضع فيروس في برامج مشهورة مثل مايكروسوفت وورد وكانت تباع هذه البرامج بسعر (1.5) دولار ويقوم الفيروس بتدمير البيانات وترك رسالة «مرحباً بكم عند دونجون ـ أمجد وباسيت ألفي» وكانت الأقراص التي تباع للأمريكان فقط هي الحاملة للفيروس والسبب كما يقول باسيت «بسبب أنكم متقرصنون يجب أن تعاقبوا» وتم اعتبار هذا التصميم من الفيروسات العالية المهارة».

لقد سرقت العصابات الروس من الولايات المتحدة الأمريكية وحدها (5) مليار دولار. وافادت ال (FBI) ان العصابات الروسية مشتركة مع (290) دولة ذات اتصال مع أكثر من (1000) شركة إجرامية، ويسرقون ويبيعون تصاميم، وأسرار، ومنتجات من مختبرات البحث والتطوير العلمي، قامت (FBI) بملاحقة احد القراصنة الروس الذي نجح في تحويل (400.000) من حسابات سيتي بنك في الولايات المتحدة، إلى فنلندا، والمانيا، وإسرائيل، ونيوزيلاندا، وروسيا، وسويسرا (Girard, 1998)

التهديدات (Threats):

من الصعب ربط التهديدات الفضائية بمكان أو زمان، أو جماعة، فقد تصدر من هاو أو من طفل أو محترف، أو جماعة إرهابية، أو جماعة تنافسية، أو استخبارات أجنبية. ولقد حددت وكالة مشاريع البحوث الدفاعية المتقدمة (DARPA) مهددات البناء التحتي المعلوماتي وصنفتها في (5) فئات هي:

1- التهديدات الخارجية المحايدة (Exterrnal Passive Attack) (مثل التنصت، تحليل الإشارات، تحليل الذروة).

2- التهديدات الخارجية النشطة (External Active Attack)، (مثل الدخول غير المصرح به، الحمولة الزائدة، الازدحام).

3- الهجوم على نظام عامل (Running System Attack).

4- الهجوم الداخلي (Internal Attack).

5- الهجمات للوصول إلى تعديل النظام (مثل خرق حماية الدخول للنظم، والانكشاف) (DARPA, 1997, Apperdix C).

الثغرات (الانكشافات) الجديدة (New Vulnerabilities)

يقول روبرت مارش (Robert M. Marsh) رئيس اللجنة الرئاسية لحماية البنية التحتية الحساسة في رسالة إلى الرئيس الأمريكي بل كلينتون :

«إن هناك قدرة كبيرة لاستغلال الثغرات في البنية التحتية (المعلوماتية)، وإن المقدرة في تحقيق الأذى من خلال شبكات المعلومات يمثل واقعاً فعلياً، وأنه في زيادة وبمعدلات خطرة، ولدينا القليل للدفاع»(PCCIP, 1997, p. vii)

وتقول اللجنة في مقدمة تقريرها إن:

«البنية التحتية الحساسة تقف خلف كل جزء من حياتنا، إنها تشكل الأساس في رفاهيتنا، ومدعمات دفاعنا، والحارس لمستقبلنا، إنها قوة لكل جزء من مجتمعنا، ولا توجد أولوية ملحة أكثر من أولوية توفير الأمن، والاستمرارية، وتوافر البناء التحتي الحساس (PCCIP, 1997, p. vii)

إن أي فوضى في البناء التحتي المعلوماتي ستكون مربكة، ويمكن أن تؤدي إلى نتائج خطيرة على الاقتصاد، والأمن، والحياة الاجتماعية. إن الاعتمادية المتبادلة والترابط المتبادل جعل احتمالية أن تكون المعلومات، والبنية التحتية المعلوماتية منكشفة احتمالية عالية.

لقد دعا رئيس توجيه حماية البنية التحتية المعلوماتية المعروف (PDD-63) بمجهود وطني لتأمين الأمن للبنية التحتية الأمريكية التي أصبحت عالية الانكشافات ومترابطة، وتشمل البنية التحية المعلوماتية (الأمريكية)، الاتصالات، والبنوك والمال، والطاقة، والمواصلات، والخدمات الحكومية الأساسية، قال مدير وكالة المخابرات الأمريكية

(CIA) في الواشنطن بوست 1996/6/26م. «لدينا الدليل بأن عدداً كبيراً من الدول في العالم تطور الخطط والاستراتيجيات والأدوات لشن هجمات معلوماتية على الحاسبات المتصلة بالجيش الأمريكي».

إن التهديدات الفيزيقية والفضائية حقيقة، فالعمليات الإرهابية الموجهة ضد الممتلكات، والمؤسسات، والسفارات، والتجمعات السكنية كثيرة، ولا تتوقف التهديدات الفيزيقية على الإرهاب بل تشمل الكوارث الطبيعية كالفيضانات، والأعاصير، والهزات الأرضية، والزلازل بالإضافة إلى ذلك فإن التهديدات الفيزيقية على مستوى الأفراد (كاستخدام القنابل) لا تتوقف خطورته على ما يحدثه من خراب وتدمير، وأنما يتعدى ذلك إذا كانت العملية موجهة ضد مؤسسات تحوي مواد كيمائية، أو بيولوجية، أو نووية.

ويمكن أن تستخدم التعديات الفيزيقية على خطوط الهاتف، أو خطوط المياه، أو محولات الطاقة، أو محطات تحويل الطاقة، أو الميكروويف، أو أبراج الاتصالات. فقد يقتحم اللصوص المعلومات في المكاتب، والعمائر بمساعدة مخطط الطابق، أو عن طريق أسماء العاملين والبيانات الأخرى التي حصلوا عليها عن طريق السرقة، كما يسرق اللصوص البرامج التجارية من الشركات، وعلى سبيل المثال أُخبر ماتيكروفان عام 1997 بأن اللصوص المسلحين قد تمكنوا من سرقة (100000) قرص ليزر (CD) تقدر قيمتها بـ(906) مليون دولار من ضمنهم تومبن ليتوا (Thompen Litho) في أسكتلندا.

ويركز بعض اللصوص الهجمات على الأوراق والوثائق، والأقراص، وبعضهم يسرقون أجهزة الكمبيوتر ـ قد خسرت فيزا (Visa) التحكم على (314000) من حسابات بطاقة الائتمان عندما أخذ سارق الكمبيوتر الذي كان يعمل على شحن أنواع بطاقة الائتمان.

تشكل سرقة الكمبيوترات ومكوناتها خطر اً منخفضاً، ولكنها جريمة كبرى من الناحية المادية ـ كما يذكر (Toronto Globe & Mail) بأنه طبقاً «لقول البوليس فان معظم السارقين يقومون على التكتيك «الكسر والقبض» بعد كسر نوافذ الطابق الأرضي يحملون الكمبيوترات بمقدار (20000) دولار ، وأجزائها، والعملية كلها لا

تأخذ أكثر من دقيقتين. ويشكل الكمبيوتر المحمول (Lap Top) الهدف الرئيسي للسرقة لأنه صغير الحجم، وخفيف في الوزن.

أما الثغرات الفضائية (Cyber Vulnerabilities) والناجمة عن زيادة الاعتمادية على الاتصالات والمعلومات فقد زادت احتمالية التعديات على البنية التحتية المعلوماتية. ولقد توصلت اللجنة الرئاسية لحماية البنية التحتية (المعلوماتية) الحساسة إلى أن حماية البنية التحتية الحساسة يتطلب فهماً للثغرات الأمنية، والعمل على خفض وإغلاق هذه الثغرات، ولقد أوصت اللجنة بأن لا يكون الانتظار لحدوث كارثة استراتيجية خطيرة، الآن هو الوقت المناسب للقيام بحماية المستقبل.

وقدرت وزارة الدفاع الأمريكية من خلال وكالة (DISA) الأمريكية (53) تعدياً عام 1992م، و(115) تعدياً عام 1993، و(255) تعدياً عام 1994، و(559) تعدياً عام 1995، والشكل التالي يبين التطور في التعديات على وزارة الدفاع الأمريكية، وهناك من يقدر أن حماية النظم الأمنية الأمريكية يتراوح بين (18إلى15) مليار دولار (Report to Congressional Requesters, 1996).

تتفاوت البنى التحتية المعلوماتية بدرجة انكشافها إلى الكوارث الطبيعية، والإهمال البشري، وسوء التصرف الإنساني. ولقد حدد التقرير الرئاسي الأمريكي بخصوص حماية البنية التحتية الحساسة (PCCIP, 1997) خمسة قطاعات بناءً على الخصائص المشتركة لها، وهذه القطاعات هي :

1- قطاع الاتصالات والمعلومات (Information and Communication)، ويشمل شبكات الاتصالات العامة (PTN)، والانترنت، والحاسبات في المنازل، والاستخدام الأكاديمي، والحكومي، والتجاري.
2- قطاع التوزيع الفيزيقي (Physical Distribution)، ويشمل الطرق السريعة للمواصلات، وخطوط السكك الحديدية، والموانئ، وخطوط المياه، والمطارات، وشركات النقل، وخدمات الشحن التي تسهل انتقال الأفراد والبضائع.
3- قطاع الطاقة (Energy)، ويشمل الصناعات التي تنتج الطاقة، وتوزع الطاقة الكهربائية، والبترول، والغاز الطبيعي.

4- قطاع المال والبنوك (Banking and Finance)، ويشمل البنوك، وشركات الخدمات المالية من غير البنوك، ونظم الرواتب، وشركات الاستثمار، والقروض المتبادلة، والتبادلات الأمنية والمادية.

5- قطاع الخدمات الإنسانية الحيوية (Vital Human Services)، ويشمل نظم التزويد بالمياه، وخدمات الطوارئ والخدمات الحكومية (البطالة، والضمان الاجتماعي، وتعويض الاعاقات، وإدارة سجلات المواليد . . . إلخ.).

1- قطاع الاتصالات والمعلومات :

يشمل قطاع الاتصالات والمعلومات شبكات الاتصالات العامة (PTN)، والإنترنت، وملايين الحاسبات في المنازل، والاستخدامات الحكومية، والأكاديمية، والتجارية، ويشمل الاتصالات العامة، وشبكاتها، الشبكات المحلية، وشبكات التلفونات، وشبكات الخلوي، والستالايت، ويشكل حوالي (2) مليون ميل من الألياف الضوئية، والنحاسية التي تعد الهيكل العظمي لقطاع الاتصالات والمعلومات.

التهديدات : إن ثبات وأمن قطاع الاتصالات والمعلومات قد أصبح موضوعاً في غاية الأهمية، وإن المهدد الرئيس لثبات الاتصالات والمعلومات هو الكوارث الطبيعية وإخفاقات النظام. أما المهدد الرئيس للأمن فهو التعديات المتعمدة الفيزيقية أو الفضائية (Cyber) على الحاسب ونظم المعلومات والبناء التحتي المعلوماتي. ويعتمد على الاستعدادات الحكومية لمواجهة الكوارث الطبيعية في حماية ثبات توافر خدمات الاتصالات والمعلومات. أما المهدد الثالث فهو التعديات المتعمدة واعتماداً على الهدف أو الأهداف من التعدي فربما تكون التعديات بهدف السرقة أو التعديل، أو الاستخدام، أو التخريب، أو التدمير للمعلومات والبيانات المخزنة، أو الحرمان من الخدمة (DOS).

يشمل المعتدون منظمات الاستخبارات الوطنية، وناقلات المعلومات، والإرهابيين، والمجرمين، والمنافسين التجارين، والدخلاء، والداخلين غير المنتمين حيث يشكل الداخليون الشريحة الكبيرة المهددة للأمن ولنظم المعلومات، وهناك الكثير من التعديات على الحاسب ونظم المعلومات التي لا يتم كشفها. ويستخدم المهاجمون وسائل متنوعة ضد البنية التحتية المعلوماتية بما في ذلك تحليل الذروة، والهجمات

المشفرة، والجهمات الفنية، والهجمات الفيزيقية، والهجمات الفضائية. وأهم هذه الهجمات وأكثرها خطورة الهجمات الفيزيقية والفضائية. لقد زادت الثغرات في البناء التحتي المعلوماتي في التسعينات، وأصبحت أكثر عرضة للتعديات الفيزيقية.

الشغرات : إن عمل شبكة الاتصالات العامة يشكل انكشافاً (ثغرة) للتعدي الفضائي، وهناك العديد من نقاط الدخول لهذه الشبكة، فكل نقاط التحويل والتبديل ونظم التشغيل عرضة للاعتداء. ومما يجعل الدخول للنظام والمعلومات سهلاً اتاحة التفصيلات الفنية عن النظام، والتبادلات المفتوحة، وبروتوكولات الاتصالات. إن دخول طرف ثالث للنظام (أجنبي) يشكل تهديداً. كما أن الثغرات تشمل البدالات (Switching) مثلما حصل مع شركة (AT & T) الأمريكية عام 1990 عند حصل تغير في البدالات أدى إلى فشل في (114) نظام إلكتروني. وتشمل التهديدات الدخول عن بعد، والتغير أو التحكم من قبل أشخاص مهرة، كما أن التغير في معدات النقل (Transport) بين البدالات، ومكاتب التوزيع داخل الشبكة يشكل تهديداً.

إن غالبية الشبكات الضوئية (Sonets) تدار عن بعد من خلال شبكات رزم البيانات والمعرضة للدخول الإلكتروني. أما شبكات بروتوكول اشارات القناة العامة المعروف (Common Channel Signaling [CCS]) فهي شبكات بيانات غير متصلة تحمل تعليمات التجهيز للملقمات، والخدمات الخاصة، والفواتير. إن تعطيل البرامج الخاصة بذلك في اشارات القناة العامة (CCS) يمكن تصورها فيما حدث عام 1991 في خدمات الهاتف في عدة مدن أمريكية منها (6.7) مليون خط في واشنطن دي سي والتي تعطلت لعدة ساعات بسبب مشكلة في بروتوكول اشارات القناة العامة-(CCS) الناجم عن طباعة حرف بالخطأ في رمز البروتوكول. كما أن عمليات الشبكة المتعلقة بالتحكم (Control) مكشوفة للتعديات.

وأخيراً تشكل إدارة الاتصالات ثغرة أخرى، فعمليات تشغيل الاتصالات وصيانتها، وإدامتها تعتمد على برمجيات ونظم دعم، ونظم عمليات الدعم عرضة لعدد من التعديات، حيث يمكن للمعتدي أن يؤخر أو يستجيب، أو يمزق الطلب الذي تم تلقيه، ويمكن أن يغير المهاجم في محتويات طلب الصيانة بحيث يؤثر في مواصفات مستوى الإدارة للعقد، ويمكن عمل الصيانة عن بعد مما يجعلها عرضه للدخول غير المصرح به.

2- قطاع التوزيع الفيزيقي للبنية التحتية

يعد التوزيع الفيزيقي للبنية التحتية هاماً للأمن الوطني، وللاقتصاد، والتنافس الدولي، ولنوعية الحياة. إن الترابط الكبير لشبكات الطرق، والسكك الحديدية، والموانئ، والمياه، والمطارات، والخطوط الجوية تسهل الانتقال الفعال للبضائع والسلع، والناس. ويشكل النقل عنصراً رئيسياً في الاقتصاد الأمريكي حيث قدر عام 1995 بحوالي (777) مليار دولار أو (11%) من إجمالي الناتج المحلي (GDP)، وتعتمد التجارة الأمريكية بشكل خاص على التصدير والاستيراد، ونقل المواد الخام، والسلع، والغذاء، والمعدات.

يشمل التوزيع الفيزيقي التحتي في الولايات المتحدة (4) مليون ميل من الطرق العامة والسريعة، وأكثر من (360) ألف من شركات النقل بين الولايات، و(20) مليون شاحنة تستخدم لأغراض الأعمال، و(190) مليون سيارة شخصية، وخطوط طيران تنقل أكثر من نصف مليار مسافر سنوياً من خلال (400) مطار. ويشمل (1900) ميناء، و(1700) مرفأ نهري على (11) ألف ميل من الطرق المائية التي تحمل مختلف السلع، كما يشمل (1.4) مليون ميل من خطوط البترول والغاز الطبيعي، ويشمل خدمات البريد، وغالبية البناء التحتي في النقل مملوكة للقطاع الخاص، في حين تملك الحكومة الفدرالية نظام الطيران الوطني (NAS)، والذي يدار من قبل إدارة الطيران الفدرالية (FAA)، والجسور التي تدار من قبل الجيش.

الثغرات والتهديدات :

النقل عرضة لعدد من التهديدات الفيزيقية مثل الكوارث الطبيعية، والفيضانات، والهزات الأرضية، والانفطارات، والأعاصير، وعند حدوث هذه الكوارث تساهم الحكومة والقطاع الخاص، والقطاع التطوعي في إعادة الخدمة، كما تعد التهديدات البشرية والإرهابية من أكثرها خطورة.

3- قطاع الطاقة :

تشكل الطاقة الدم الذي يغذي البنى التحتية المعلوماتية التي تقوم عليها نظم الأمن، والاقتصاد، والرفاهية الاجتماعية المترابطة . ويتكون البناء التحتي للطاقة من

ثلاث صناعات تنتج، وتوزع الطاقة الكهربائية، وهي نظم الطاقة الكهربائية، والبترول، والغاز الطبيعي.

التهديدات : تشمل التهديدات لنظم الطاقة الحكومات العدائية، والجماعات الإرهابية، والجماعات المنظمة، والأفراد، والموظفين المسرحين، والدخلاء، والكوارث الطبيعية، والحوادث. وهناك مئات التعديات التي تقع على نظم الطاقة وقدر أن (75-80%) من الحوادث الأمنية تقع من قبل موظفين داخل المنظمة. بالإضافة إلى تعطيل نظم الطاقة أو تدميرها (البرمجيات والتعدي الفيزيقي) وأشكال الحرائق، والمصافي، وخطوط البترول.

الثغرات : تشمل الثغرات في قطاع الطاقة المجالات التالية :

1- الطاقة الكهربائية : نظم مولدات الطاقة، ونظم الإرسال، ونظم الانتاج، والتحكم الإلكتروني.

2- البترول والغاز الطبيعي : الموردات، والنقل، والتخزين، والتوزيع، وتشمل الثغرات التي تواجه صناعة الطاقة، وهي الثغرات الناجمة عن بيئة العمل والمتعلقة بهياكل النظم المفتوحة، والعمليات المركزية، والاتصالات عبر الشبكة العامة، والصيانة عن بعد، وكذلك ثغرات نظم الإشراف وزيادة المعلومات عن الثغرات، وزيادة توافر التقنيات المتقدمة.

4- قطاع المال والبنوك :

يعد النظام المالي مركزياً في التجارة المحلية والدولية، وفي الحياة اليومية للناس. وعلى سبيل المثال فإن البنوك الأمريكية تملك حوالي (4.5) ترليون دولار، وهناك (3) ترليون دولار عمليات يومية، وحوالي (10) مليون وظيفة. وهناك أكثر من (1) مليار بطاقة ائتمان في الولايات المتحدة مسؤولة عن (500) مليار من المشتريات السنوية. ويعد البناء المالي وقطاع البنوك مكوناً من خمسة قطاعات رئيسة هي البنوك، وشركات الخدمات المالية، ونظم السحب (الدفع)، وشركات الإستثمار، والتبادلات المادية والأمنية.

التهديدات : إن أهم المهددات الحالية للنظام المالي هو تهديد فيزيقي بما في ذلك الكوارث الطبيعية، أو التعدي المباشر المتعمد على الثغرات الظاهرة في النظام. وتزداد

هذه التهديدات مع التوافر في المعلومات عن طريق الإنترنت واللازمة لمثل هذه التعديات، وعلى المستوى المؤسسي فإن أكبر مهدد أمني هو الداخليون والذين ربما يستخدمون وصولاً غير شرعياً إلى المعلومات السرية أو نظم التشغيل من أجل المنفعة، بالإضافة إلى التهديدات الفضائية من قبل المجموعات الإرهابية أو الدخلاء.

الثغرات : هناك ثغرات فيزيقية في النظم المالية ناجمة عن الاعتماد العرضي للنظم المالية (المؤسسات المالية، والأوراق النقدية، وسوق الأسهم).

5- قطاع الخدمات الإنسانية الحيوية

يشمل قطاع الخدمات الإنسانية الحيوية (Vital Human Services) ثلاث بنى تحتية وهي مزودات المياه، وخدمات الطوارئ، والخدمات الحكومية. وهناك من يضيف إلى ذلك الغذاء، والرعاية الصحية، وقوة العمل كبنى تحتية حرجة إضافية. وتختلف البنى التحتية الثلاث عن البنى الأخرى المسماه البنى الحرجة لأنها تقع مسؤوليتها على الدولة، وتتعامل مع الحاجات الإنسانية والأمن.

ويتكون نظام المياه من خمسة عناصر هي : مصدر المياه، ومعالجة المياه، ونظام الفتح والتخزين والأنابيب . . . إلخ، ونظام التوزيع الذي يحمل الماء بصورته النهائية، وجمع المياه العادمة ونظام المعالجة.

أما استخدامات المياه فمتنوعة منها الزراعية، أو الصناعية، أوالعمل، أو الاطفاء، أو الاستخدام المنزلي. ويجب أن يتوفر الماء عند الطلب ويرسل بضغط مناسب، وأن يكون آمناً للاستخدام. والأفعال التي قد تؤثر في هذه العوامل الثلاثة يمكن أن تضعف البنية التحتية.

كما أن تلويث المياه، وتلويث مصادرها يمكن أن يحدث بالصدفة، أو لأسباب طبيعية، وانتشار الطفيليات (Parasites)، ويمكن أن تزرع هذه الطفيليات بشكل قصدي لتسبب الأمراض والموت، وهناك أنواع من البكتريا والفيروسات التي يمكنها البقاء حتى بعد إضافة الكلور للماء. إن تلويث المياه بأي شكل متعمد يشكل تهديداً كبيراً. كما يمكن تخريب مضخات المياه مما يعني عدم وصولها إلى المشتركين، ويمكن تعطيل عمل الإطفاء للحرائق في حالة عدم توفر المياه لإخماد الحرائق. كما أن تعطيل نظام التوزيع يؤدي إلى عدم وصول المياه للمساكن وأخيراً فإن عدم وصول المياه إلى الصناعة والزراعة سيؤدي إلى نتائج سلبية وخسارة كبيرة.

يشمل البناء التحتي لخدمات الطوارئ الإطفاء، والشرطة، والإنقاذ، وخدمات الطوارئ الطبية. وهذه الخدمات معنية بإنقاذ الأرواح والحياة البشرية. ويؤثر التعدي على هذه الخدمات سلباً في أداء هذه الخدمات ويسهم في فقدان حياة الناس، وينجم عن ذلك خسارة مادية كبيرة.

وسائل التعدي على البنية التحتية المعلوماتية

1- الناس: الداخليون (Insiders) والخارجيون (Outsiders)

الداخليون هم الموظفون والأفراد ممن يعملون داخل المنظمات الرسمية والخاصة، وأفراد المجتمع عامة، كلا الفئتين تشكلان تهديداً كبيراً للبنية التحتية المعلوماتية، حيث يمكن أن تستغل معلومات المنظمة، أو يتم تخريبها بغرض الانتقام، أو تدمير بنيتها الفيزيقية، أو الحرمان من استخدامها. وتشمل شرائح الداخليين الخونة (Traitors)، والعملاء (Moles)، وعلاقات العمل (المصالح)، والزيارات، والطلبات، وهذا يشمل الحصول على المعلومات من الداخليين، وفي غالبية هذه الحالات فإن الداخل يستفيد من توافر المعلومات التي يمكن أن تستخدم في المنافسات التجارية، أو العسكرية، أو السياسية، أو في مصالح أخرى. كما يشمل الاحتيال (Fraud)، والتزوير (Embezzlement) حيث يستغل الداخليون مصادر المعلومات للفائدة المالية، أو الاستخدام المهين لهذه المصادر (Degrading). أما الخارجيون فتمثل أخطارهم في التعديات على أنظمة المعلومات، والدخول غير المشروع، وممارسة الإرهاب ... إلخ.

هل سيحل الدخلاء محل الجنود في المستقبل عند اندلاع الحروب؟ وهل ستكون الحروب في المستقبل بلا دماء؟ يمكن وضع استخدام بندقية من نوع (HERF) لتخريب نظم الاتصالات، والطاقة، وشبكات المياه ... إلخ من أي شخص من داخل المجتمع. ويمكن استخدام المجسات والأسلحة الذكية لتدمير البناء التحتي المعلوماتي، وخاصة مراكز الاتصالات، والتلفزيون، والراديو، والصحف .... إلخ. يمكن أن تكون حروب الغد حروباً بلا جيوش. ويمكن تعطيل نظم المال، والبنوك، والطيران المدني ، والطاقة من أي فرد عادي يملك وسائل بسيطة في التخريب.

ولقد ذكر أركويلا، ورونفلدت (Arquilla & Ronfeldt) في مقالتهم (Cyberwar is Comming) أن مفهوم حرب الفضاء «تعني حرب الفضاء، حرب المعلومات» . . . يعني التنفيذ والإعداد لتنفيذ عمليات عسكرية بناءً على المبادئ المرتبطة بالمعلومات ويؤدي إلى تعطيل إن لم يكن التدمير للمعلومات ونظم الاتصالات بما في ذلك الثقافة العسكرية حيث تقوم عليها شرعية القتال والنظام . . إلخ. يشكل الدخلاء غير الشرعيين للبناء التحتي المعلوماتي، ولنظم المعلومات عامة جزءاً من الصراع العرقي والإقليمي والدولي. وتقوم الأطراف بشن هجمات معلوماتية كل على الطرف الآخر، وفيما يلي مجموعة من الأمثلة على ذلك (Arquilla & Ronfeldt, 1996).

صادرت مجموعة نادي الدخلاء الباكستاني (Pakistani Hackers Club) موقع إيباك (AIPAC) (لجنة العلاقات العامة الأمريكية ـ الإسرائيلية) وحولوا الموقع من موقع لمؤيدي إسرائيل إلى موقع ضد إسرائيل وتمكنوا من خرق قاعدة بيانات إيباك وسرقوا (700) رقم بطاقة ائتمان للداعمين الأقوياء اليهود لإسرائيل، وقد أرسلوا إلى (3500) من أعضاء إيباك رسائل تبين استغلالهم.

بالمقابل فإن جماعة حماس وحزب الله قد استخدموا سياسة رمي الحجارة الإلكترونية (Virtual Electronic Stones) والتي يسميها الجانب الفلسطيني الجهاد الإلكتروني (e-Jihad). (Bodrchgrave; Gilluff; Cardash, and Ledyerwood, 2000). والتي تتمثل في مهاجمة المواقع الالكترونية لإسرائيل، أو تحويل محتواها إلى مادة دعائية لصالح الطرف المهاجم أو سلبية ضد أصحاب الموقع.

إن رصد الرئيس كلينتون لمبلغ (2) مليار لمكافحة الإرهاب الفضائي (Cyberterrorism)، والحرب الفضائية (Cyberwars) في المستقبل ولتعزيز أمن الحاسب مؤشر على أن التهديدات الكونية التي تواجه الولايات المتحدة فعلية. إن تكنولوجيا الفوضى والتدمير في تطور سريع والحكومات لازالت تعتمد على تكنولوجيا قديمة. والتطور التكنولوجي في الـ(10) سنوات القادمة يساوي التطور التكنولوجي في القرن العشرين بأكمله. ومن الناحية الاقتصادية، فإن الجريمة الفضائية تهدر المليارات من الدولارات، وكما قال جوشكافيشر (Fischer) في مؤتمر برلين الذين شمل خبراء الإنترنت من الدول الثمانية الكبار (الصناعية) (G8) ان الخسارة التي سببتها الجريمة الفضائية وصلت (42.9) مليار دولار للدول الثمانية الكبار بما في ذلك الولايات المتحدة الأمريكية، وهذه بلا شك مجرد البداية (Girard, 1998).

2- المعدات والأدوات :

البنادق الإشعاعية بنادق (HERF) وهي بنادق ذات ترددات إشعاعية عالية (Hig Energy Raidion Frequency) تؤدي إلى الحرمان من الخدمة (Denial of Service) للعديد من الخدمات. وهذا السلاح بسيط التركيب ويعتمد على حجم قوة المصدر المستخدمة، والمدى أوالدقة المطلوبة. ويمكن تصميمها بأشكال وأنواع مختلفة. وتقوم هذه البنادق بتوجيه الإشارات الإشعاعية العالية إلى الأهداف المحددة مسبقاً. والدوائر الكهربائية أكثر عرضة لأن تحمل حمولة كهرومغناطيسية زائدة مما يؤدي إلى تعطلها، وهذا ما يمكن استغلاله من بنادق (HERF).

وببساطة فإن بنادق (HERF) ما هي إلا مرسل راديو يشبه المرسلات المضيئة في أعلى الأبراج والتي تحذر الطائرات من الاصطدام بها، وتعمل العديد من التقنيات الحديثة مثل جهاز الحاسب المحمول (Portable)، أو الجوال (Cellularphone) بمستويات طاقة منخفضة. وتعمل هذه البنادق من خلال التصويب على الهدف وتحميله طاقة زائدة تؤدي إلى تعطيل إرساله. فمثلاً يمكن أن تعطل عمل الحاسب أو شبكة حاسبات، أو تلفونات . . . إلخ. حيث إن هذه المعدات مصممة بمستويات طاقة متدنية (Low-level)، وعندما تضاف إلى دوائرها حمولة زائدة، لا تستطيع العمل وبالتالي تتعطل أو تتوقف مرحلياً (Schwartau, 1994).

قنابل إرسال النبض الكهرومغناطيسي (Electromagnetic Pulse Tranformer Bombs [EPTB]) وهي تشبه بندقية ال(HERF) إلا إنها أكثر قوة بمقدار (1000) مرة. إنها قوية جداً لدرجة إنها تعطل الدوائر والشرائح في الحاسب والمعلومات المخزنة بحيث لا يمكن إصلاحها.

ومن تطبيقات قنبلة (EPTB) تخريب الأدوات الاتصالاتية، والتحرش بالخصم، وتعطيل الاتصالات، والتدمير والتخريب للخدمات الإلكترونية، والإرهاب، أو ضد الإرهاب، والدفاع الأرضي الجوي، وتدمير المعدات الإلكترونية، والتي تعمل بالطريقة نفسها التي تعمل بها بندقية (HERF)، إلا إنها أكثر فعالية وقوة من هذه البنادق، وأن التدمير الذي تحدثة يبقى مستديماً وغير مؤقت كما هو الحال بالنسبة لبنادق (HERF).

لقد أظهر تقرير وكالة إدارة الأزمات الفدرالية أن الأجهزة التالية من المرجح أن لا تعمل في حالة تعرضها إلى القنابل الكهرومغناطيسية (EPTB)، وهي الحاسبات، والتيار الكهربائي للحاسبات، ومزودات الترانستسترات، ومكونات أشباه المواصلات وتؤدي إلى إيقاف عمل الكوابل الكهربائية، ونظم الإنذار (Alarm Systems)، ونظم

الاتصالات المباشرة (Intercom Systems)، ومعدات تلفونات الترانزستورات المرسل والمستقبل، ونظم ضبط القوة، والاتصالات . . . إلخ.

وفي عام 1982م حول الخلاف بين بريطانيا والأرجنتين على جزر الفوكلاند، وبصاروخ واحد موجه من الحاسب اكسوكت (Exocet) والبالغة قيمته (200) ألف دولار، دمرت السفينة الحربية ـ المدمرة البريطانية شيفيلد البالغة قيمتها (50) مليون دولار. هذا النوع من السلاح مبرمج ومغذىً بمعلومات سابقة عن الوضع التضاريسي، وعن مكان الهدف، ويصعب التمويه عليه، ويصيب هدفه بدقة، وبالتالي يمكن الاستغناء عن الكثير من العسكر في هذا المجال.

3- الإرهاب.

تتعرض البنية التحتية المعلوماتية للعمليات الإرهابية بكافة أشكالها سواء كان الإرهاب التقليدي (Conventional Terriorism) والذي يقوم على تدمير البناء التحتي المعلوماتي الفيزيقي كالمباني وأجهزة الحاسب، وتعطيل المواصلات . . إلخ. أو الإرهاب التكنولوجي (Technologgical Terriorism) والذي يهدف إلى التأثير على الفضاء باستخدام وسائل مادية مثل تفجير محطات الطاقة، والاتصالات مما يؤثر على الفضاء التخيلي (Cyberspace)، أو الإرهاب الفضائي (Cyber Terriorism) والذي يقوم على تدمير البرمجيات وتدمير المعلومات، ويشمل الفئات التالية:

1- التعدي الفضائي (Cyber attacks) على قاعدة معلومات محددة، وهذا يشمل دخولاً غير شرعي على الشبكة أو النظام يهدف إلى تحويل مالي بطريقة غير قانونية، وسرقة ممتلكات معلوماتية، وتحطيم الملفات.

2- التعدي الفضائي يهدف الحصول على وصول إلى الشبكة والاستفادة من إجراءات الأمن واستغلال الثغرات فيها.

3- التجسس.

4- غلق النظام.

5- تعليمات مؤذية مثل القنابل المنطقية، وحصان طروادة لتدمير البرمجيات (Girard, 1998).

كما يمكن أن يستخدم الارهابيون الشبكة الكونية في تنظيم اتصالاتهم وعملياتهم واستغلال المواقع مثل المواقع الاباحية لاخفاء معلوماتهم، كما أن استخدام تقنيات الحماية مثل التشفير تزيد عملهم أمناً. ولا يتوقف الخطر عند استخدام الارهابيون للبنية التحتية المعلوماتية الكونية، بل أنها تسهل حصولهم على المعلومات والبرمجيات التي تساعدهم في تنفيذ أعمالهم مثل تصميم الأسلحة، وتحضير الأسلحة البيولوجية

وغيرها.

لقد ذكر تقرير «الحاسبات في خطر» عام 1991 الصادر عن مجلس البحث القومي أن «الارهاب المستقبلي ربما يكون قادراً على استخدام لوحة المفاتيح أكثر من استخدامه للقنبلة»، أما تقرير الجريمة الفضائية (Cybercrime) والارهاب الفضائي (Cyberterroism) والحرب الفضائية (Cyberwarfare) عام 1998 والصادر عن مشروع الجريمة المنظمة الكونية التابع لمركز الدراسات الدولية والاستراتيجية - فذكر أن الجماعات الارهابية تحاول انهاء وجود أمريكا كدولة عظم (Denning, 2000 a).

وتستخدم القاعدة، وحماس، وحزب الله الشبكة في التواصل مع اعضائها وفي تنظيم نشاطاتها. وقد استخدم حزب الله ثلاث مواقع مع الشبكة هي (www.hizbollah.org) وهو الموقع الرئيسي (الاعلامي)، وموقع (www.moqawama.org). وهو لنشر أخبار المقاومة والاهداف الاسرائيلية والثالث للاخبار والمعلومات (WWW.almanar.Com.Lb). أما جماعة (Aum Shinrikyo) والمسؤولة عن حادثة مترو الانفاق في طوكيو التي توفي فيها (12) وجرح (6000) فقد استخدمت التشفير لحماية معلوماتها والتي بينت نيتها فياستخدام اسلحة التدمير الشامل في اليابان والولايات المتحدة (Denning, 2000 b).

4- الارهاب المعلوماتي Informational Terrorism

هناك طريقتان يوظف بهما الارهاب وهجوم إرهاب معلوماتي: 1- عندما تكون تقتية المعلومات (IT) هدف و/أو، حيث تشمل هذه الطريقة استهداف الارهاب لنظم المعلومات بقصد التخريب الالكتروني أو المادي، مدمراً أو مخلاً لنظم المعلومات وأي بنية تحتية معلوماتية (مثل الطاقة والاتصالات). 2- عندما تكون تقنية المعلومات إداة لعملية كبيرة، وتشمل هذه الطريقة انتقاء الارهاب واستغلاله لنظام المعلومات أو سارقاً للبيانات أو مجبراً للبيانات، على أداء مهمة غير شرعية (مثل التقاط ضبط حركة الطائرات).

	ارهاب فيزيقي	ارهاب رقمي
الاداة فيزيقية	أ. ارهاب تقليدي	ج. هجوم IRAفي لندن عام 1992
رقمية	ب. قرصنة (التقاط نظام حركة السطرة الجوية لاسقاط طائرة)	د. حصن طروادة في مقاسم الشبكات العامة

المصدر: Devost, Houghton, & Pollard, 1998

الفصل الثالث

خصائص المجتمع المعلوماتي

مقدمــة

تسعى المجتمعات الإنسانية إلى الوصول إلى الاتزان الاجتماعي في كافة نظمها الاجتماعية وذلك لتحقيق الأمن الاجتماعي فيها لكي تتمكن من أداء وظائفها . وتتطور مع ذلك مهددات الأمن الاجتماعي بجوانبها المتنوعة والمتعددة، والتي تتطور مع تطور المجتمعات الإنسانية. ففي المجتمع الزراعي ساد الشجار كنوع من الصراع الفردي والجماعي واستخدمت العصي، والحجارة وما توافر في البيئة كأدوات في الصراع والعدوان والدفاع. وشكل الناتج الزراعي قيمة عالية (هدفاً ذا قيمة عالية) ينافس عليه الناس، مما جعل الثروة مقاسة بالملكية الزراعية، وجعل منها مصدر تهديد بقاء، ونشبت بسببها الخلافات، والصراعات، والحروب على المستوى الفردي، والجماعي، والدولي. واصبحت الارض هي مصدر القوة (power). وفي المجتمع الصناعي حلت الآلة الصناعيــة محل المواد الأوليــة الزراعيــة ومحل الإنســان، واستخدمت الأدوات الصناعية كالبندقية في الصراع مع الآخرين (أو في ارتكاب الجريمة)، وفي الحروب. وأصبحت التجارة والصناعة من الأهداف التي تجلب الكثير من المال وبالتالي جعلت الناس، والدول يتنافسون على الحصول عليها، وظهرت المستعمرات، وسيطرت الدول على مقدرات بعضها بعضاً، وخاصة على المواد الاولية اللازمه للصناعه واصبح المال هو المصدر الرئيس للقوة (البداينة، 1998 ب).

إن التطورات الاجتماعية والاقتصادية ونوعية النشاط الاقتصادي خاصة تحدد الكثير من الأنماط السلوكية في أي مجتمع. وتماشياً مع النمط الاقتصادي الإنتاجي وما يواكبه من تغيَّر في سلوكيات الأفراد، يتطور الأمن ليواجه مشكلات جديدة وفق الأساليب المتاحة ووفق النمط الاقتصاد السائد. أما المجتمع المعلوماتي بما يحمله من أنماط جديدة من السلوكيات، وحيث يعتمد الاقتصاد على المعلومات فقدأصبحت متطلبات الأمن مختلفة ومهدداته مختلفة، فأساس النشاط الاقتصادي والاجتماعي الآن ليس (البرونز ولا الحديد كما في العصور السابقة) وإنما المعلومة (البداينة، 1999 أ)، ولذلك فإن مصادر التنافس والصراع وادوات الصراع والحروب تعتمد على المعلومات بدرجة كبيرة، لابل أصبحت المعلومات ادوات صراع لقد اصبحت المعلومات مصدر القوة.

لقد قدم توفلر (Toffler) أنموذجاً في التطور التكنولوجي وصف فيه عصر الزراعة حيث رأى أن هذا العصر قد اتصف بالعمالة اليدوية، وركز الانسان فيه على جمع

الغذاء اللازم للحد الأدنى للمعيشه. وخلال هذا العصر كان التطور التكنولوجي محدوداً، وبطيئاً، وكان هناك سوء فهم حتى لغالبية المفاهيم العلمية، وشاع استخدام وسائل مبسطة في الاتصال منها العدائية، والرسائل من خلال الخيول، والطيور، والإعلام ووسائط الرؤية الأخرى. واستمر لفترة زمنية قصيرة، وكان لدخول محركات البخار والتي حلت الآلات الميكانيكية بدل القوة العضلية للإنسان والحيوانات. لقد بدأ عصر المعلومات وفق رؤية توفلر عام 1955م، والتي كانت السنة الأولى التي يقوم فيها أصحاب الياقات البيضاء بأعمال أصحاب الياقات الزرقاء، وحيث تمت المعرفة بشكل كبير. ولقد شرعت تطور الاتصالات والتكنولوجيا خلال عصر المعلومات من خلال الستالايت، ووصلات الألياف الضوئية. (Boni, & Kovacich, 1999).

ولقد تطورت الجريمة وفق نمط النشاط الاقتصادي فمثلاً جريمة السرقة كانت في المجتمع الزراعي، فأن السرقة قد كانت من البنك، أو من الناس، أو من المحلات، وكان وسيلة الهروب فيها الهروب على الأقدام أو على ظهر الخيل، مع ملاحظة محدودية المكان الذي يمكن أن يهرب إليه الشخص، وحتى تتم السرقة فإن ذلك يتطلب معرفة بركوب الخيل، والمكان (الهدف) والطرق المؤدية إليه والخطة. وإذا لم يتوفر الحصان (الوسيلة) فإن مجرم السرقة قد يتحول إلى سرقة الناس بدل البنك. أما في المجتمع الصناعي فقد زادت السيارة من سرعة وقدرة السارق على الابتعاد عن مكان السرقة، ومكنت السارق من سرقة أكثر من بنك أو محل تجاري أو شخص، كما توسعت مناطق السرقة وابتعدت عن مكان السرقة بمسافة أكبر مما كان في المجتمع الزراعي، وقد وفرت الطرق السريعة سرعة الابتعاد عن منطقة السرقة كلها. أما المجتمع المعلوماتي فإنه ليس للسارق حاجة إلى السيارة، ولا إلى الابتعاد عن المكان، حيث يمكن له أن يكون في المنطقة ذاتها، أو في منطقة بعيدة جداً عن مكان البنك أو الحاسبات التي يمكن أن يسطو عليها، ويمكن أن ينقل المسروقات إلى حسابات في بلدان بعيدة، وذلك من خلال استخدام الشبكات والإنترنت وبعض المساعدات من البرمجيات الخاصة بالدخول غير المشروع إلى حسابات العملاء في البنك وتحويلها من حساب لآخر أو إلى حساب في بنك في دولة أخرى.(Kovacich, & Boni, 2000).

وتحتل المعلومات مكاناً مركزياً في مجتمع المعلومات (Informational society)، والتي أثرت في البنى الاقتصادية والاجتماعية والسياسية للمجتمعات. مما أثر في أنماط السلوك والقيم الإنسانية والثقافية. حيث شاع الانتشار الثقافي وعولمة الثقافة، والاقتصاد، و الجريمة. وعلى الرغم من الاختلافات في مستويات التطورات

الاجتماعية في المجتمعات إلا أن سيادة آليات وبنى الاقتصاد ستكون متشابهة في المجتمعات الكونية (الكاملي 1998).

ولم تدخل الدول والمجتمعات إلى هذا العصر فارغة اليدين بل إن الكثير منها قد استعد منذ فترة طويلة لدخول هذا العصر لكي لايُسبق من المجتمعات الأخرى وتتراجع مكانته العالمية. فدولة مثل بريطانيا ترى اضمحلال مصادرها الاستراتيجية في عصر المعلومات، قد أعدت خطة طوارئ للحاق بالمعلومات رصد لها حوالي (50) مليون جنيه (Simons, 1983). وقبل أكثر من (20) عاماً وضعت اليابان وثيقة شهيرة أسمتها (مجتمع المعلومات عام 2000) كخطة وطنية لإيجاد مكان مناسب لليابان بين الدول في عصر المعلومات، مما أدى إلى ردة فعل غربية فورية تمثلت في خطط وطنية واستراتيجيات ومشاريع كلها هدفت إلى التحضير لعصر المعلومات ودخوله بأمان. فعلى سبيل المثال وضعت فرنسا خطة ديجول (1972) والمعروفة باسم (Plan Cacul) وتقرير نورامينك (Nora-Minc) عام (1978)، أما انجلترا فوضعت تقرير ألفي (Alvey) عام (1982م). ووضعت السوق الأوربية (1980) تقرير دبلن (Dublin) والولايات المتحدة وضعت تقرير روكفللر (Rochefeller) عام (1976) وتقرير سالمون (Salmon) . أما كوريا الجنوبية فوضعت كونجرس تنمية التكنولوجيا المتقدمة (1982)، وتايوان (1980) الخطة العشرية لصناعة المعلومات واليونسكو (1974) برنامج نظم المعلومات الوطنية (NATIS) (علي، 1994). بالإضافة خطط لدول مثل السويد وكندا في تحويل مجتمعها إلى معلوماتي.

وللتقنية دور هام في تطور مجتمع المعلومات، وهي استخدام وسائل مفيدة ناتجة عن تطبيق المعرفة العلمية في الحقول المختلفة، وتشمل المنتوج الانساني المادي كالسيارات والطائرات، والإنارة، والطرق، والحاسب، والإنترنت، وقواعد المعلومات. . . . الخ. إن المتتبع لتطور التقنيات في مجالات الحياة العامة ليدرك الفجوة الكبيرة في هذه التطورات قبل وبعد الحرب الكونية. ومع كل تطور تقني كان الإنسان يوظف ذلك لتحصين أمنه واستتبابه، فلقد استخدم الإنسان النار كإشارات في الحرب، ولقد انتقل استخدام الإنسان مما هومتاح في البيئة وتطويعه في صيانة أمنه كالبيوت، والتحصينات، والحواجز، والقلاع إلى استخدام التقنيات لأغراض مختلفة منها الاستخدام الأمني.

إن التطورات في علوم كثيرة وخاصة الإلكترونيات قد ساهمت في تطور التقنيات وأدى إلى نقل العالم بأسره إلى عصر المعلومات. فتطور الإلكترونيات من الصمامات

المفرغة (Vacum tube) إلى الترانسيستور فالدوائر المتكاملة (IC) ثم الدوائر المتكاملة المتسعة (LSI) أدت جميعها إلى ثورة علمية في وسائل الاتصال والبحث العلمي وذلك بفعل ما تمتاز به هذه التقنيات من موثوقية في الأداء، وفي توافر الخصوصية في الاستعمال، وفي حجم الإنجاز، ومستوى الأداء وفي خفض الكلفة (بكري، 1991). فعالم الغد كما يتخيله جيتس سيعتمد على الطريق السريع في المعلومات والذي سيلغي المسافات، وان سوق المعلومات الكونية ستكون هائلة وستجمع الطرق المختلفة التي يتم فيها تبادل المعلومات والسلع والأفكار الإنسانية. وتمر المجتمعات كافة بتغيرات هائلة في تغير نمط ابنيتها الاجتماعية والفكرية، فالبريد الإلكتروني مثلا والإنترنت يمران بالحلقة ذاتها التي مر بها الهاتف في الاتصالات ذات الاتجاهين، فهذا الغازي للبيوت، والمزعج سرعان ما أصبح رفيق الأفراد في كل مكان يضعه الفرد في جيبه، ويلازمه في فراشه. لقد وفر الاتصال عن بعد الوقت، واختصر المسافات. في المجتمع المعلوماتي تربط آلات المعلومات ذات الفعالية العالية وتمكن الفرد من التواصل الميسور مع الناس، وتتصفح الكتاب من أي مكتبة وأنت جالس خلف شاشة حاسبك، ويصبح من الممكن أن ترشدك الكاميرا المسروقة من شقتك بمكانها بالضبط، وفي أي مدينة هي.

لقد يسرت التقنيات في مجال الاتصالات بالذات عملية التواصل بين الأفراد، ولم يعد من الضروري أن يكون الاتصال وجهاً لوجه (F2F)، بل أصبح الاتصال عن بعد ممكناً وشائعاً. لقد وفر استخدام التقنيات الوقت والجهد البشري، وساهم في توفير الوقت، ورفع الإنتاجية، وتقريب المسافات، ونشر الثقافات.

إن عمليات الانتقال للبنية التحتية للمجتمعات (Infrastructural Transformation)، قائمة في أغلب المجتمعات وتنتج عن الأثر المدمج للتطور التكنولوجي المبني على تكنولوجيا المعلومات وظهور اقتصاد المعلومات الدولي وعمليات التغير الثقافي والظاهرة بشكل واضح في تغير مكانة الإناث في المجتمع وظهور ا لوعي البيئي. ويعتقد كاستلز (Castells, 1996) أن سقوط الاتحاد السوفياتي ما هو إلا نتيجة عدم قدرته على ادارة التحول إلى مجتمع المعلومات ، ويؤكد كاستلز على الصفة الاجتماعية لتكوين المعلومات (Informational Society) والتي هي أبعد من أثر تكنولوجيا المعلومات (Castells, 1996). إن الاكتشافات التكنولوجية الرئيسة 'المعالج الرقيق" عام1971، وإعادة توحيد الـ(DNA) 1973م، والحاسب الشخصي 1974-1976م، وتكوين الإنترنت وانتشارها في السبعينيات والثمانينيات. كل هذا وغيره قد أظهر أن المعلومات عنصر أساسي في عملية انتقال المجتمعات إلى هذا العصر.

يمتاز المجتمع المعلوماتي بأنه يركز على العمليات التي تعالج فيها المعلومات وأن المادة الخام الأساسية هي المعلومة، وبالتالي فإن المعرفة تؤدي إلى تولد معرفة جديدة وهذا عكس المواد الأساسية في المجتمعات الأخرى حيث تنضب المواد الأساسية بسبب الاستهلاك، أما في مجتمع المعلومات فالمعلومات تولد المعلومات (Kelly, 1994)، مما يجعل مصادر المجتمع المعلوماتي متجددة ولا تنضب.

يقول نيكوس كازانتزاكس (Kazantzakis) في كتابه (Report to Greco) عبارة تتضمن لغة حينية قديمة وتقول (عليك لعنتي، لتعش في عصر مهم) ويبدو أن الجميع ملعونون وفرحون في هذا العصر، ويرى فريدمان (Friedman) أن هذا العصر قد بدأ مع نهاية الحرب الباردة أي تاريخ هدم جدار برلين (تشرين أول عام ١٩٨٩) وأما عصر المعلومات فبدايته شبكة الانترنت، فمن الانغلاق (جدار برلين) إلى الانفتاح (شبكة الانترنت). هذا العصر عمره سنوات معدودة، اختفت الاسس القديمة للنجاح (السيطرة على الموارد الطبيعية) أما الآن فإن أساس النجاح هو امتلاك المعلومات، وكما يقول بيل جيتس فإن " خيال الانسان يمثل الأصول الوحيدة التي تملكها شركتنا" أي شركة مايكروسوفت والتي قيمتها السوقية (470) مليار دولار امريكي، وهذه القيمة لا تشكل أكثر من 1-2٪ من قيمتها في السوق (بينيس، 2001).

معايير المجتمع المعلوماتي

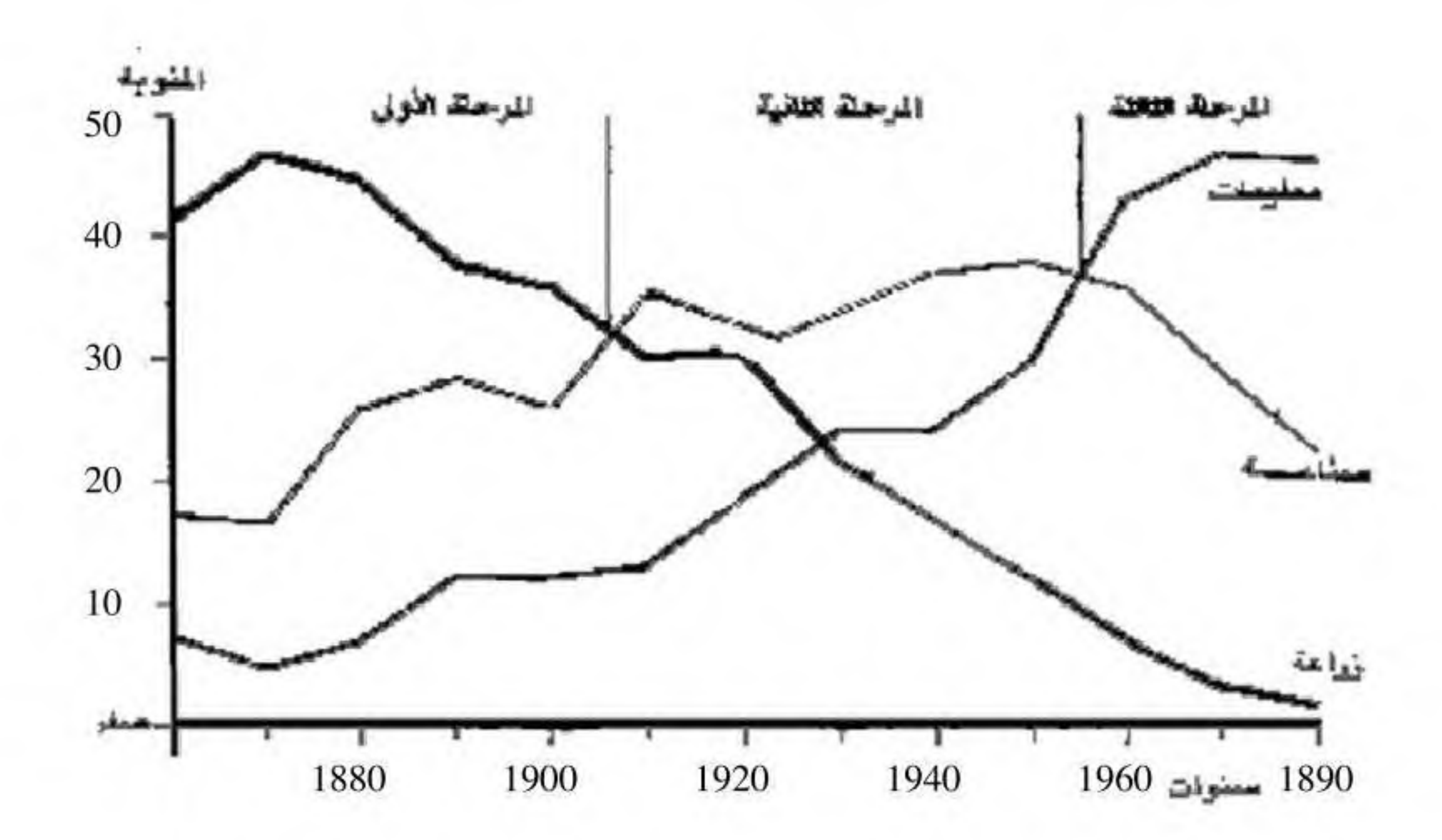
تمثل معايير المجتمع المعلوماتي قياسات يمكن من خلالها التنبؤ بدخول المجتمع، أو تحوله، أو تطوره إلى مجتمع معلوماتي أو مقدار النمو البنائي للمجتمع كمجتمع معلوماتي. ويمكن النظر إلى تكوين البنية التحتية المعلوماتية للمجتمع ومدى نضوج هذه البنية كمؤشر على كون المجتمع مجتمع معلوماتي. ومن أساليب قياس معلومات المجتمع عدد الحاسبات أو عدد الخادمات للانترنت، أو عدد المشتركين، وأمية الحاسب، ونسبة مساهمة المعلومات في إجمال الدخل القومي، وتوزيع العمالة على القطاعات الاقتصادية الرئيسة . . . إلخ. ولقد بدأ اعتماد البعد التقني كأساس لقياس التنمية.

حدد مارتن خمسة معايير للمجتمع المعلوماتي هي: المعيار التقني، والمعيار الاجتماعي والمعيار الاقتصادي، والمعيار السياسي، والمعيار الثقافي. (1) المعيار التقني ويمثل المعيار التقني الاعتماد المتزايد على تقانة المعلومات كمصدر للعمل والثروة والبنية التحتية والاعتماد المتزايد والكبير على التقنيات وخاصة تقنيات المعلومات، والتي هناك من يصف هذا

العصر بأنه عصر الانفوبديا. (2) المعيار الاجتماعي فيبرز أهمية المعلومات في تحسين شروط الحياة، ونشر استخدام الحاسب والاستفادة من المعلومات وتوظيفها في شتى النشاطات الإنسانية. وتلعب المعلومات دوراً مهماً في التنمية البشرية الشاملة (التعليم، الصحة، الغذاء، محاربة المرض... إلخ). (3) المعيار الاقتصادي ويركزعلى دور المعلومات في الاقتصاد، بحيث يصبح الاقتصاد اقتصاد معلومات، وتزداد التجارة الإلكترونية كمؤشر على ذلك، وتصبح المعلومات مصدر ثروة وسلعة، ومصدر اقتصاد مهم، وتكوين فرص عمل جديدة. حيث برز الاقتصاد الإلكتروني، والعملة الإلكترونية، والتحويل الإلكتروني، والأعمال الإلكترونية. إنه باختصار اقتصاد المعلومات، أي الاقتصاد المتجدد دائماً. (4)المعيار السياسي ويركز على زيادة وعي الناس بأهمية المعلومات في اتخاذ القرارات ومشاركتهم في صنع القرار السياسي، واستخدام المعلومات في الاقتراع والتصويت، والانتخاب، وزيادة الوعي الاجتماعي من خلال جماعات النقاش التي تتجاوز الحدود الوطنية، وتكوين جماعات ضغط سياسي. وأخيراً (5) المعيار الثقافي ويركز على تكوين نظام قيم معلوماتي فيه تركيز على القيم الثقافية الداعمة للمعلومات (احترام الرأي واحترام حقوق الآخرين واحترام الملكية الفكرية) (Martin, 1988). ولقد حدد وبستر (Webster, 1995) خمسة خصائص للمجتمع المعلوماتي وهي الخصائص التالية: 1- التقني (Technological)، 2- الاقتصادي (Economic)، 3- المهني (Occupational)، 4- الفضائي(Spatial)، 5- الثقافي (Cultural).

قبل عام (1989) لم يكن هناك تجارة الكترونية أما في عصر 1998 فقد بلغت (43) مليار دولار ومن المتوقع أن تصل إلى (1.3) تريليون دولار، وكان أفضل عشرة أسهم قابلة للنمو يمكن امتلاكها هي التي تعود لشركات الطاقة، والمصارف والصناعة، أما اليوم فإن أفضل عشرة موسسات في بورصة الاسهم تعود لمؤسسات تقانية المعلومات مثل (Dell, Cisco, sun) (Qualcomm, EMC, Intel) ولقد كان الامازون (Amazon) مجرد اسم نهر في البرازيل أما اليوم فهو أكبر متجر كتب على الانترنت وتحول من اسم إلى فعل (We ve been amazoned) (بينيس، 2001)،

ويذكر علي (1994) أن المجتمع الأمريكي قد مر بثلاث مراحل تطورية هي الزراعة (1860-1906)، والصناعة (1906-1954)، والمرحلة الثالثة هي مرحلة المعلومات حيث بدأت عمالة المعلومات تفوق عمالة الصناعة وخاصة منذ عام (1954)، والشكل التالي يبين ذلك.



شكل رقم (2) توزيع عمالة المجتمع الأمريكي بين القطاعات المختلفة

المصدر : (علي، 1994، ص. 276)

إن عدم التيقن من خصائص المجتمع المعلوماتي مازال قائماً، ولابد من إعادة بناء نماذج نظرية جديدة مناسبة لتفسير العمليات الاجتماعية الحديثة فيه. إن مجتمع المعلومات يمكن وصفه بأنه تدفق وانسياب (Flows) للمعلومات يتم من خلال الشبكات من المنظمات والمؤسسات وهذا التدفق والانسياب يمثل سلسلة صادقة مكررة مبرمجة من التبادل والتفاعل بين المكانات المادية (الفيزيقية) غير المتصلة والمحتلة من الفاعلية الاجتماعية في المنظمات الرسمية والمؤسسات الاجتماعية. وتعمل محددات انسياب الشبكات في البناء الاجتماعي من خلال أربعة مستويات هي :

1- تنظيم شبكات مواقع الفاعلين والمنظمات والمؤسسات في المجتمع وفي الاقتصاد.

2- وجود اختلافات هامة داخل الشبكة وبين الشبكات فيما يخص الأهمية البنائية للانسياب الحاصل في تلك الشبكات لأهداف نظام ما.

3- تفاوت القوة بين المكانات داخل كل شبكة.

4- إن منطق الانسياب عالمي وليس شمولياً (Castells, 1996, P. 29).

إن السيطرة والتحكم في المعرفة والمعلومات تحددان من يملك القدرة في المجتمع، فالتكنوقراط هي الطبقة المسيطرة بغض النظر عن من يمارس السلطة السياسية، ويصبح التكنوقراط والخبراء والمهنيون هم أدوات التغيير في المجتمع المعلوماتي. إن محرك

البخار لم يؤدي وحده إلى ثورة صناعية ولكن بدونه لم يكن من الممكن وجود مجتمع صناعي (Mokyr, 1990) وبدون المعلومات، وشبكات الإنترنت وشبكات حاسبات، ومراكز البحوث لن يكون هناك مجتمع معلوماتي.

ويرى كنيدي (موثق في العمر، 2000) أن نشوء المجتمع المعلوماتي كان بسبب العوامل التالية:

1- الانفجار السكاني، حيث تضاعف سكان العالم مرات، لقد احتاج العالم إلى (123) سنة ليصل إلى الملياري نسمة عام 1927م واحتاج إلى (12) سنة ليصل إلى (6) مليار نسمة عام 1999م، ومع هذه الزيادة الكبيرة للسكان تتناقص المصادر الاقتصادية والغذائية، مما أدى إلى الالتفات إلى المعلومات والدراسات للبحث عن بدائل لخفض السكان، وايجاد بدائل للغذاء.

2- التعدي على البيئة، وشمل التدمير المتعمد وغير المتعمد للبيئة، وخاصة في الدول الصناعية وما تحدثه الصناعة من تلوث للبيئة، وخاصة في مجال طمر النفايات النووية تحت الأرض، أو في المياه مما أثر على طبقة الأوزون، فزيادة تهديدات البيئة دفعت إلى البحث عن وسائل الحماية والتعاون الدولي، ووضع الاتفاقيات التي تحول دون تخريب البيئة.

3- التقانة البيولوجية، حيث التطورات الهائلة في هندسة الجينات والتوصل إلى الخريطة الوراثية للإنسان، وما نجم عن التطورات في هذا الحقل وخاصة في مجال الاستنساخ، مما أدى التطور في جانب المعلومات، ودعم البحوث وأثارت قضايا أخلاقية وإنسانية في هذه الجوانب.

4- زيادة الفجوة بين الشمال والجنوب، هناك عدة عوامل ساهمت في اتساع الفجوة بين الدول الغنية والنامية، منها زيادة السكان في الدول النامية، والفساد، وشح المصادر، والديون، واستغلال ثرواتها من قبل الدول الغنية، مما زاد مشكلاتها الاجتماعية كالفقر، والجريمة، والتخلف.

لقد حدد جودارد (Goddard) أربعة عناصر مترابطة في الانتقال إلى مجتمع المعلومات وهي:

أ ـ احتلال المعلومات لمرحلة مركزية «كمصدر استراتيجي» مما يعتمد عليه الاقتصاد العالمي، حيث تعتمد التجارة الدولية البينية على الاتصالات والشبكات الإلكترونية وفيها المعلومات عنصر أساسي لهذه النشاطات .

ب ـ تقنيات الحاسب والاتصالات وفرت البناء التحتي الذي يمكن من معالجة المعلومات وتوزيعها بسرعة ودقة .

ج ـ النمو المضطرد لقطاع «تجارة المعلومات» من الاقتصاد وولادة الكثير من التقنيات الجديدة مما يجعل هذا السوق في تجدد مستمر.

د ـ نمو اقتصاد «المعلومات» الذي أدى إلى التكامل الوطني والمحلي للاقتصاد. وذلك من خلال الانتقال السريع للعمليات التجارية المتبادلة وسرعة الانجاز والتواصل بين الوحدات الاقتصادية المختلفة محلياً ودولياً (Goddard, 1992).

خصائص مجتمع المعلومات

لكل نمط من المجتمعات خصائصه وبناه الاجتماعية والاقتصادية والسياسية التي تميزه، فللمجتمعات الزراعية خصائصها، وللمجتمعات الصناعية خصائصها، وللمجتمع المعلوماتي خصائصه. إن التغيرات في البناء الاجتماعي للمجتمعات تسهم في التأثير على سلوكيات الناس وشخصياتهم وتتطور البنى الاجتماعية والاقتصادية والسياسية تبعاً لذلك. وغني عن القول أن استخدام التقنيات قد سهل الحياة الاجتماعية، ورفع الأداء ووفر الوقت والجهد. ويمكن أن تحل الإنترنت مثلاً مشكلة التسوق التقليدي، والبحث عن المواقف، والنقل، ومرافقة الإناث خاصة في المجتمعات المحافظة إلى الأسواق، حيث لايستدعي التسوق المستقبلي هذه المرافقة. إلا أن آثار هذه التقنيات قد تركزت في عولمة الاقتصاد والاعلام، والثقافة، وعولمة الجريمة، والمخدرات. فلم تعد السيادة الوطنية كما هي الآن حيث الأقمار الصناعية التي تكشف أدق الامور على الارض وما في جوفها. والاشارات التلفزيونية التي تدخل البيوت والحدود دون استئذان. والأطباق التلفزيونية (الدشات) قد استباحت السيادة المنزلية قبل السيادة الوطنية، وأصبح المجتمع العالمي مجتمعاً واحداً. ويمكن تحديد أهم الخصائص البنائية والعمليات التفاعلية للمجتمع المعلوماتي في الأتي:

عصر المعلومات عصر امريكي، حيث يساهم الاقتصاد الامريكي بـ ٢٨٪ من الناتج المحلي الاجمالي العالمي، وان غالبية ادوات المعلومات هي ادوات امريكية مثل الحاسب، والانترنت، والأجهزة الرقمية الشخصية، ولغة عصر المعلومات هي الانجليزية بالاضافة الى وجود نظام تعليمي جامعي وعالي جيد، ونظم تشغيل الحاسبات "ميكروسوفت وندوز" وتقبل العمال للتقنيات الجديدة، ان عصر المعلومات عصر الفوضى المسيطر عليها (كوهين، 2001).

يتسم عصر المعلومات بثلاث سمات هي: (1) تغيرات كمية في مقدار المعلومات المتدفقة ونوعيتها (2) ارسال المعلومات للعديد من الاطراف (بشر، أو آلات)، و(3) انشاء الشبكات ، ففي مجال تراكم المعرفة الكمي والنوعي الكبيران يؤثران في الامن القومي، حيث يمكن التعامل مع ميدان المعركة بالعبور ومع مساحة متر او أقل. أما ارسال المعلومات للعديد من الاطراف فيمكن توضيحها من خلال انتقاء الصاروخ لهدفه من خلال التغذية المسبقة له بالمعلومات اللازمة. وأخيراً فان ميزات الشبكات توفر التواصل من خلال البريد الالكتروني والاتصالات ونقل المعلومات ويتم تبادلها بين الاطراف وبشكل سريع جداً دون المرور بالبيروقراطية الهرمية. (كوهين، 2001).

أولاً: الخصائص التقنية

1-**البنية التحتية المعلوماتية الوطنية** ((National Information Infrastructure (NII)

تعرف البنية التحتية المعلوماتية «بأنها الهيكل الفيزيقي والتخيلي للمجتمع المعلوماتي» وتشمل الحد الأدنى من العناصر التالية :

1- الشبكات المالية والمستخدمة في نقل المعلومات بين المؤسسات المالية.

2- شبكات المؤسسات والشركات الخاصة والمستخدمة في تبادل المعلومات بين مثيلاتها الدولية.

3- شبكات الخدمة العامة كالتلفونات ووسائل الاتصالات الأخرى.

4- الشبكات المتعاونة مثل شبكات المنظمات التعليمية متبادلة المنافع كما هو الحال في الإنترنت.

5- شبكات الاشتراك وهي مؤسسات قطاع خاص خدماتية في مجال المعلومات مثل الشبكات المحلية ومتصلة مع بعضها البعض لتقديم خدمات معلوماتية.

6- الشبكات الحكومية والدفاعية وتستخدم لأغراض الاتصالات الحكومية والعسكرية مثل شبكات وزارات الدفاع والتي تعرف أحياناً بـ (Command, (C3I) Control, Communication & Intelligence.

7- شبكات وحدات الخدمات العامة التي تعتمد على الحاسب كالمياه والمجاري والمواصلات ونظام المرور.

8- شبكات المعلومات التي تعتمد على الحاسب مثل التحكم بالبيئة والأمن في المباني الكبيرة (Devost, 1995)

ويحدد ديفوست ثلاث فئات رئيسة للمعلومات :

1- المعلومات العسكرية (Military Information)، وهي المعلومات التي تتعامل مع التطورات العسكرية، وأسرار العمليات العسكرية، والاستخبارات، ونظم التحكم، والمراسلات بين كبار الضباط، وملفات العسكر، والنشاطات العسكرية عامة والمراسلات الدنيا.

2- معلومات الأعمال (Business Information)، والتي تشمل السجلات الخاصة بالأعمال، والعمليات البنكية، وسجلات الأفراد المالية، ونظم الأعمال، والعمليات المالية الأخرى.

3-المعلومات الشخصية (Personal Infromation) وتشمل معلومات عن الأفراد في مجالات الائتمان، والنظم الشخصية (الأحوال المدنية) الملفات والاتصالات بين الأفراد (Devost, 1995).

إن التعدي على المؤسسات العسكرية، أو مؤسسات القطاع الخاص وخاصة البنوك يكلف الدولة الكثير من المال لإعادته إلى وضعه السابق، فمثلاً تقدير العمليات المالية في سوق وول ستريت (Wall Street) وحده بأنه تجاوز الترليون دولار (USGAO, 1995). أما التعدي على نظم المعلومات العسكرية وخاصة ما يتعلق بنظم الدفاع المعقدة، فإن ذلك يؤدي إلى كلفه باهظة قد تودي في أوقات الحروب إلى هزيمة الدولة، كما أن تدمير المعلومات الشخصية كالأحوال المدنية أو سجلات الأفراد يؤدي إلى تعقيدات أمنية كبيرة.

ولا تتوقف العمليات والتعديات ضد المعلومات وتدميرها أو تخريبها فقط، وإنما سرقتها، حيث ظهر ما يسمى الإرهاب الفضائي (cyber terrorism)، و سرقة أسرار القنبلة الذرية أو الجرثومية أو سرقة تصميم طائرة الشبح (Stealth)، أو الصورايخ العابرة للقارات، أو القنابل الذكية . . . إلخ. هذه الأسرار العسكرية تكلف مليارات الدولارات ويمكن أن تسرق بثمن زهيد، و بشكل ميسر ودون كلفة تذكر.

2- المعلوماتية (Informatics):

يمتاز المجتمع المعلوماتي بأنه يركز على العمليات التي تعالج فيها المعلومات وان المادة الخام الأساسية هي المعلومة، وبالتالي فإن المعرفة تؤدي إلى تولد معرفة جديدة وهذا عكس المواد الأساسية في المجتمعات الأخرى حيث تنضب المواد الأساسية بسبب الاستهلاك، أما في مجتمع المعلومات فالمعلومات تولد المعلومات (Kelly, 1994).

إن معنى المعلومات الذي يتبادر إلى الذهن هو معنى لغوي في طبيعته، وهو أن المعلومات ذات معنى مفيد، لها موضوع ولها علاقة بالذكاء، أو بتعليمات عمل شيء ما. وإذا ما طبق هذا المعنى للمعلومات على المجتمع المعلوماتي، فإنه يصار إلى البحث عن خصائص المجتمع المعلوماتي والمتمثلة في الاقتصاد والثقافة . . . إلخ.

وكما يقول ستونر (Stonier) **بأن :**

«المعلومات موجودة، وهي ليست بحاجة إلى إدراكها أو فهمها لكي يثبت وجودها. إنها لا تتطلب ذكاءً لتفسيرها، وليس بالضرورة أن يكون لها معنى لكي تكون موجودة . . . إنها موجودة» (Stonier, 1990, p. 21).

المعلومات رمز شاع استخدامه من الانفجار المعلوماتي، إلى الثورة المعلوماتية إلى المجتمع المعلوماتي إلى الحرب المعلوماتية. والمعرفة تجريد عام، وهي ضرورية للتطبيق وعمليات الإنتاج. قد تكون المعرفة (كما في الكتاب المنهجي) محمية بقوانين حقوق النشر ولكن ما يحويه الكتاب من معرفة ليست ملكاً لأحد. إن المواصفات والتصميم لمنتج ما نتيجة لعملية تطبيق المعرفة العامة في مشكلة محددة لإنتاج معلومات مملوكة. فالمعلومات هي أداة للتطبيق وهي نتيجة بالمحصلة لتلك العملية. المعلومات ذات خصائص مشتركة، فالمعرفة عالمية في صفاتها، والمعلومات محددة والبيانات (Data) ضرورية. فأي كتاب يتكون من بيانات (أحرف، كلمات . . .الخ). وهذه البيانات يمكن أن تكون أرقاماً، رموزاً، . . .الخ. ويمكن التمييز بين المعرفة والمعلومات والبيانات على النحو التالي:

إن الناظر إلى البيانات يراها بسهولة ولكن ليس بالضرورة أن يرى معانيها خاصة في غياب نظام الحروف التي تشكل الكلمات وبالتالي تشكل الجمل، وهذه البيانات تصبح معلومات، ومن بين المعلومات الأفكار، المفاهيم، المعاني . . . الخ، بينما نظام اللغة (التي كتب فيها الكتاب) صنع من الإنسان ويفهم من قبله وهذا يماثل مستوى المعرفة التامة (Curry, 1997).

في مجتمعات اليوم هناك كميات هائلة من الثروة المجتمعية يتم تطويرها، أو تخزينها، أو نقلها، أو انتقاؤها باستخدام وسائل نقل المعلومات وتخزينها كالحاسب، فالصناعة الأمريكية وحدها تحول (Transmit) مليارات الدولارات من العمليات المالية يومياً من خلال الشبكات الالكترونية.

مثلما ارتفعت البني الاقتصادية في المجتمعات من الزراعة إلى الصناعة إلى ما بعد الصناعة، فالمعلومات والتكنولوجيا تابعت ارتقاءها مع المادة من الصلابة (المعادن) إلى الهش (الفحم، والبخار) إلى المائع (النفط والسائل) إلى الليونة (المعلومات). هذا التتالي في المادة في صورة عناصر لا مادية ولامحسوسة شمل التقسيم التالي :

1ـ البيانـات (Data)

2ـ المعلومات (Information)

3ـ المعــارف (Knowledge)

4ـ الذكـاء (Intellignce) (علي، 1994، ص 46).

ولكل من هذه المكونات أنظمة خاصة به فمثلاً نظام معالجة البيانات ونظام معالجة المعلومات . . . الخ. وهذا ا لترتيب لهذه المكونات من البسيط إلى المعقد وكل منها يشكل نقلة نوعية خاصة تشكل البيانات الأساسية التي تتولد منها المعلومة وهي الأرقام أو الكلمات وتمثل المعلومات البيانات. أما المعارف فهي حصيلة التكامل بين المعلومة والمدركات الحسية. و نرى أن الذكاء يمثل الطاقة الذهنية لدى الإنسان والتي يدخرها الانسان ويطورها بالتعليم.

3- التخيلية (الافتراضية) (Virtualty)

ويمكن تصور مجتمع المعلومات اليوم كمجتمع تخيلي (Virtual Society)، يرتبط بطريق المعلومات السريع (Information Highway) أو كما وصفه جيتس بأنه طريق المعلومات فائق السرعة (Information Superhighway) وهذا الطريق كما تخيله جيتس (Gates, 1995/1998) فيه التفاعلات المعرفية والمعلوماتية، والاجتماعية، والسلوكيات تاخذ أنماطاً مختلفة تماماً عما اعتدنا عليه. وقد بدأ هذا العصر فعلاً فمتاجر الإنترنت العربية الإلكترونية بدأت بشركة الزهور المصرية (www.egyptflowers.net)، وانترنت بوكيه في لبنان (www.internetbouquet.com.lb) كأول متجرين عربيين لتوزيع وبيع الزهور الحقيقية، وما لبثت حتى انتشر استعمال الإنترنت في الصحافة، والشركات والدوائر الحكومية، وحتى المؤسسات الأمنية كالامن العام والشرطة والمخابرات (الخميس، 1997)، ثم امتد ذلك إلى المقاهي التخيلية، فلم يعد سبب ذهابك للمقهى (بما كان يحمل من وصم اجتماعي سلبي) هو ذات ا لسبب اليوم، حيث تدخل إلى طريق المعلومات السريع وتسبح في الفضاء الخارجي بانسياب وتتصفح محتويات الكتب، وتسمع الموسيقى وتشتري وتبيع، وتسافر بلا جواز سفر أوتصريح دخول. لا بل ستكون الأمور أكثر صعوبة في التخيل عندما لاتكون بحاجة إلى الهاتف العادي أو الكهرباء لتدخل إلى العالم فحاسب الطاقة الشمسي، والتلفون

الجوال ستمكنك من التسوق أو البحث أو السفر أو الحجز لتذكرتك أو فندقك وانت في مزرعتك أو في رحلة صيد أو في سيارتك أو حتى في غرفة نومك أو أي مكان في العالم. فلم يعد الهاتف متنقلاً (جوالاً)، والمكتب أو العمليات المالية، أو المراسلات، بل أصبح الإنسان «محمولاً» "متنقلاً" فبجهاز واحد بحجم كف اليد مثل أجهزة المفكرة الشخصية (PDA) أو الأجهزة التي تعمل بنظام بالم (Palm) يمكن الشخص التواصل مع الإنترنت، وإرسال، واستقبال المكالمات (الجوال) والفاكسات . . . إلخ. لقد أصبح الإنسان رقمياً متجولاً.

هذا بالاضافة إلى الكثير من التطبيقات العملية الأخرى وخاصة الطبية، فالطبيب يمكن أن يحمل أحد أجهزة المفكرة الشخصية وتحوي قاعدة بيانات لمرضاه ولأنواع الأدوية، يرسل ويستقبل منها، وينظم مواعيده وتشمل التاريخ المرضي لعملائه، وفي الجانب الأمني هناك تطبيقات كثيرة منها استخدام الكاميرا الرقمية. وبرامج مضاهات البصمات والصور للمجرمين واسترجاع ملفاتهم وسرعة تعميم صورهم وبصماتهم.. الخ.

إن المعلومات تؤثر في الطريقة التي يتواصل فيها الناس والتي عبر عنها نائب الرئيس الأمريكي السابق آل جور بطريق المعلومات، وقال أنها ستربط الولايات المتحدة مثلما ربطتها الطرق السريعة للمواصلات، ووصفها جيتس بأنها طريق المعلومات السريع والطريق فائق السرعة كأمثلة من آليات هذا التواصل. ويشكل الحاسب الأساس في هذه الثورة المعلوماتية، حيث يربط العالم ليكون مجتمعاً واحداً، ويصبح العالم ليس قرية كونية وإنما قرية عنكبوتية غير منتظمة الخطوط. مثلما حلت الرقائق الصغيرة والتي وفرت ملايين نقاط الاتصال الكهربائي، وحل محل التواصل نقطة بنقطة، كذلك حلت الشبكات الإلكترونية لتربط العالم بطرق متعددة في آن واحد.

لقد انتقل عصر الاتصالات بفعل الحاسب الآلي والإنترنت من بث الصوت إلى بث الرزم البيانية (Packets) والتي تشمل الصوت والصورة حيث يمكن بث أكثر من رسالة بواسطة الخط الواحد في الوقت الواحد، وهذا ما لم يُتح في السابق. في مجتمع المعلومات تتداخل الجغرافيا والثقافة والمعرفة. وفي المجتمع المعلوماتي لك أن تتخيل أنك تتسوق وترى صوراً للأشياء وتصلك الأشياء الحقيقية بعد الشراء. لم يُعد

هناك فرق بين الأنموذج المُقَلدّ والمُقلدّ (الاصل)في هذا المجتمع وعلى المستوى الوطني والعالمي هناك اندماج كبير فالخطوط الفاصلة بين الوطني والاقليمي والعالمي هشة زئبقية. في هذا المجتمع يجتمع الموظفون والادارات عبر الفيديو والحاسب، ولا مكان للمكاتب التقليدية أو السكرتيرة التقليدية أو المبني التقليدي حيث تربط الحاسبات بالفاكس بالطابعة بالجوال بالانترنت، وتصبح المؤتمرات إلكترونية ويصبح التسوق إلكترونياً وتصبح السلع إلكترونية. فلم يعد المدير بحاجة إلى سكرتير لتنظيم أعماله ومواعيده، فبرنامج الحاسب يقوم بذلك وعلى مدار السنة، ويذكره بمواعيده، وبمناسباته الهامة كعيد زواجه أو عيد ميلاد أبنائه، ويذكره بالتزاماته الاجتماعية. ولم يعد كذلك بحاجة إلى متخصص في المحاسبة فبرنامج المحاسبة والمخازن يقومان بالمهام المغذية فيهما وبفعالية ودقة عاليتين. فالمدير وأينما يذهب يذهب معه مكتبه وأوراقه ومراسلاته، ويمكن الوصول إليها في أي لحظة ليلاً أو نهاراً من مكان سكنه أو مكان زيارته أو من أي مكان في العالم وستنتشر (وقد بدأت فعلاً) الأجهزة الدفترية (Notebook) كبديل لأجهزة المكاتب التقليدية حيث أن هذه الأجهزة ذات معالجات سريعة وشاشة ملونة، ولقدبلغت مبيعات هذه الأجهزة ثلث مبيعات الأجهزة التقليدية ومن المتوقع أن تزداد مبيعاتها من (30) ملياراً عام 1996م إلى (80) ملياراً في نهاية التسعينات. تعني التخيلية في مجتمع المعلومات أنك يمكن أن تسافر في الفضاء التخيلي (Cyberspace) ذاتياً في مكانك وتشتري وتتواصل مع العالم الخارجي كما لو كان جزءاً من بيتك.

لقد حدد سلوكا (Slouka, 1995) في كتابه حرب العالمين (War of the Worlds) أن التخيلية أو ما أسماه (Cyberspace) (والحديث مركز على المجتمع المعلوماتي) أن الطريق إلى المجتمع المعلوماتي سيؤدي إلى اللاواقعية (Unreality)، وأن الإنسان في هذا المجتمع سيعاني من :

1- نهاية الواقعية (Death of Reality) أي أن الواقعية لن تكون موجودة.
2- التعدي على الهوية (The Assult of Identity) .
3-التعدي على المكان (The Assult of Place) .
4- التعدي على المحلية (المجتمع) (The Assult of community) .
5- التعدي على الواقع (The Assult of reality).

وهو يسرد قصة تبين الطريق إلى اللاواقعية.

يذكر «في عام 1990م، أفاد مراسل نيويورك تايمز والذي تابع حالة قتل مشهورة، قتل فيها رجل زوجته الحامل واتهم فيها شخصاً أسود غير معروف. لقد سأل المراسل إحدى النساء في المنطقة (جيران) عن رأيها في المأساة وقال هل تصدقين قصة الزوج ؟ وهل لك ومن خلال معرفتك بالزوج أن تعتقدي بأنه قد دبر كل ذلك ؟ أجابت المرأة، لا أدري، إنني في لهفة إلى أن يأتي فيلم عنها (المرأة القتيلة) لكي أرى كيف انتهت هذه القصة (Slouka, 1995, p.1) .

ويرى سلوكا أن هذه المرأة لم تكن مازحة، ولقد قالت ما لديها جادة فيما قالت... إنها تنتظر مسلسلاً تلفزيونياً لكي يدلها على المأساة، وبعد سنة تم عمل مسلسل تلفزيوني بعنوان "تصبحين على خير زوجتي الحبيبة : قتل في بوسطن". وقد أجاب على تساؤلات تلك المرأة. ويعتقد سلوكا أن النمو ا لمتزايد للتباعد بين الإنسان والواقع يزيد من قبولنا بالنسخ (النماذج) كما لو كانت الأصل، لقد بدأ الإنسان قبول المجرد بدل الشيء الحقيقي، ولقد زادت وسائل الاتصال الحديثة (التلفزيون، الفيديو، الفضائيات، الانترنيت ... إلخ.) الانتقال من الواقع إلى التخيل. وقد أصبح من الصعب التميز بين المكان التخيلي (Cyberspace) والحياة الحقيقية (Real life)، ففي حالة العلم يمكنك مشاهدة التمثيل التلفزيوني لحالة الاعصار كما لو كنت في ذلك المكان، فالتكنولوجيا ليست محايدة أنها تأمر سلوكياتنا وتعيد تعريف قيمنا وتعيد تأسيس حياتنا بطرق لا نستطيع دائماً التنبوء بها.

هل ستوصلنا التكنولوجيا إلى الإفلاس الأخلاقي (Moral Bankrupcy)؟ وهل من الممكن مع التطورات في تكنولوجيا الوراثة والاستنساخ أن يوصل الجهاز العصبي للإنسان بالحاسب الآلي وتحميل (Download) الشعور الإنساني إلى الذاكرة في الحاسب (RAM) وذلك لحفظها بطريقة ما؟ وفي القريب العاجل سيصبح الخط الفاصل بين الطبيعة والتكنولوجيا ثنائية خاطئة.

4- الرقمنة (Digitization)

إن توظيف الأرقام أو الرقمنة في التقنيات الحديثة أدى إلى ثورة جديدة في هذا المجال، فالكاميرا الرقمية والموسيقى الرقمية والهاتف الرقمي والكلام الرقمي والتوقيع

الرقمي . . . إلى الحاسب الرقمي، والبحث العلمي أرقام والقياس أرقام. وأن تحويل الأمواج الصوتية في الهاتف إلى أرقام مكن ملايين الأفراد من استخدام خطوط الهاتف في ربط الحاسبات وبالتالي ربط العالم بشبكة من الحواسيب.

هل تحولت الهوية الاجتماعية والوطنية إلى أرقام؟ وهل تحول الإنسان إلى أرقام. تخيل نفسك في المواقف التالية : تتصل بصديق فأنت بحاجة إلى رقم الهاتف، ترغب بزيارة صديق فأنت بحاجة إلى رقم الشارع ورقم الشقة، أو العمارة، ملفك في المخابرات (في الدول النامية) رقم، ملفك الوطني (رقم) ورخصة القيادة والهوية، وجواز السفر الرقمي، والتلفزيون الرقمي، والبث الرقمي . . . إلخ. نحن في مجتمع رقمي. تذهب إلى عواصم الدول المعلوماتية مثل لندن، أو باريس فتتنقل بين أرجاء المدنية بتذكرة (المترو) وهي رقم دون الحاجة إلى مساعدة أحد، حسابك بالبنك لم تعد بحاجة إلى حمل نقودك، وتعرضك للنشل، يمكنك بالبطاقة البلاستيكية أن تسحب من رصيدك من أي مكان وهو ماذا؟ أرقام بأرقام (رقم الحساب، رقم المبلغ (القيمة) رقم الرصيد (قيمة . . . إلخ.).

يرى وليام ديفيدو (William Davidow)، ودبليو برين آرثر (W. Brain Arthur) من أهم المبدعين في مجال الثورة الرقمية :

"أن كل شخص قد أوصل بحبل كهربائي، جميع أنواع الجماعات والدول اليائسة قد أصبحت مترابطة، وستظهر الثقافة الكونية، حيث كل واحد له الرغبات ذاتها والحاجات نفسها خلال 15 سنة» (Brochgrave & et. al., 2000 p. ii).

ويؤكد علي (1994) أن عملية الرقمنة تقوم على أساليب منها التكويد أو التشفير (Codification)، والتبسيط (Simplification) والتوصيف بدلالة السمات (الخصائص) (Feature-based Specificattion)، وتعد الرقمنة من خصائص المجتمع المعلوماتي، وذلك لأنها تشكل الأساس في عمل الحاسب وخاصة وحدات الإدخال، فاللغات في العالم ممكن أن تتحول إلى أرقام ومن ثم إعادتها باللغة المفضلة لدى المستخدم.

5- التقنية (Technology):

من أهم خصائص المجتمع المعلوماتي الاعتماد على الجانب التقني في تسيير الحياة الاقتصادية، والاجتماعية أكثر عن غيره من أنواع المجتمعات الأخرى. حيث تشكل المعلومات ومعالجتها وتخزينها ونقلها أساساً لنشاط المجتمع وتقود إلى استخدام تقنيات المعلومات ((Information Technology (IT))، وساهم في سرعة انتشار هذه التقنيات وخاصة الحاسبات الانخفاض الحاد في أسعار كلفتها، مما يسر توافرها من الناحية الاقتصادية وسهل عملية دخولها في الطباعة والألعاب والسيارات والمصانع . . . إلخ. كما كانت الآلة هي أساس العنصر الصناعي فإن الحاسب اليوم هو المجتمع المعلوماتي، أو كما وصفها نسبت «تقنية الحاسب هي عصر المعلومات، كما كانت الآلة هي الثورة الصناعية» (Naisbitt, 1984, p. 24).

قبل حوالي (50) سنة لم يكن هناك الكثير من الهواتف، أو الحاسبات، ولم تكن الشبكة العنكبوتية موجودة، أما اليوم ففي الولايات المتحدة أكثر من (180) مليون حاسب، وهناك على مستوى العالم العربي حوالي (1.3) مليون شبكة محلية، والجدول التالي يبين التطورات في التقنية الكونية.

جدول رقم (1)

التطورات في التقنيات الكونية

الفئة	1982	1996	2002
الحاسبات الشخصية	آلاف	400 مليون	500 مليون
الشبكات المحلية	آلاف	1.3مليون	2.5 مليون
الشبكات العريضة	مئات	آلاف	عشرات الآلاف
الفيروسات	قلة	آلاف	عشرات الآلاف
معدات الوصول إلى	لا يوجود	32 مليون	300 مليون
الفنيون لهجوم فضائي	آلاف	17 مليون	19 مليون
الفنيون في مجال ضبط نظم الاتصالات	قلة	1.1 مليون	1.3 مليون

المصدر: التقرير الرئاسي لحماية البنية التحتية الحساسة (PCCIP, 1997) ص9.

والسؤال المطروح هو كيف يتحدد المجتمع المعلوماتي؟، فعملية قياس تحول المجتمع إلى المجتمع المعلوماتي قد أثارت الكثير من النقاش، هل هي بوجود التقنية، أو ما سمى (Harness of New Technology)، ولكن لابد من تحديد المجتمع ذاته زمنياً (Now) وكمية التقنية (How much) وكما طرحها ويبستر (Webster, 1995) ما الكمية اللازمة من التقنية لتحديد المجتمع بأنه معلوماتي؟، هل هي الأنفاق التقني أم بالانتشار التقني في المجتمع (Diffusion)؟، وهل يقاس الانتشار بالانفاق على تقنيات المعلومات، أم بكمية المعلومات المقدمة ومداها،؟ هذا مع العلم بأن المجتمع المعلوماتي مجتمع مستمر التشكل والتغير، أنها ظاهرة غير اجتماعية (Asocial Phenomenon) (تقنية) تستخدم لتحديد واقع اجتماعي.

فمثلاً سيارة لينكولن كونتيننتال (Lincoln Continental) **فيها المميزات التالية:**

1- يسمح نظام موقع قمر صناعي اختياري للسائق بالإشارة إلى مركز انقاذ (عن طريق الضغط على زر يتسبب في طلب هاتف السيارة المركز تلقائيا) عندما تتعطل السيارة، ويستخدم المركز تقنية القمر الصناعي في توجيه وإصلاح المركبة.

2- يتحكم مراقب القيادة في نظام رافعات السيارة على محاور عجلاتها، وممتصات الصدمات، ويغير نظام عجلة القيادة الأتوماتيكية من خلال تغيير أدوات الاحساس والمراقبات لكل عجلة.

3- يتحكم مراقب هاتف الخلية في المكالمات سواء حدثت المناقشة عبر الهاتف المركب أو عبر نظام ستريو.

4- يأخذ عداد السرعة، وعداد المسافات، ومقياس الوقود منظراً ثلاثي الأبعاد.

هذا بالإضافة إلى البرمجيات التي زودت بها بعض السيارات عن الشوارع والانتقال من شارع إلى آخر، بالإضافة إلى وحدات الأمن ومقاومة السرقة والتي تستخدم مثبتات المحرك والتي تمنع الحركة وانذار التصادم ونظام وسائد الهواء والقيادة الليلية، ولا يتسع المجال لأخذ عينات كثيرة من هذه التطبيقات منها التطبيقات العلمية (علم الحياة، والفلك، والفيزياء، والرياضيات)، والتلفاز، والفيدو، والعلوم الاجتماعية (روسينبرج، 2000).

6- الفضائية السبرانية (Cyberspace)

لقد انتقل الناس من العمل على الارض الى التنافس على الفضاء، فالخيال العلمي بخصوص الزيارات المدنية للفضاء قد أصبح واقعاً، ولم تتسابق الحكومات على الفضاء لوحدها، بل انتقل الارهاب الى الفضاء لتسهيل الأعمال الارهابية التقليدية. وحتى الصراعات بين الجماعات قد انتقلت الى الشبكة العالمية، وظهرت مفاهيم جديدة مثل الجهاد الالكتروني (e-jihad)، وغيرها. لا بل قد اصبح الفضاء ملاذاً ومخبأ للجريمة فاستخدام التشفير لاخفاء المعلومات وتبادلها بين الجماعات ومنها الارهابية والجريمة المنظمة اصبح شائعاً (Denning & Baugh, Jr, 1999).

إن مفهوم «المجتمع المعلوماتي» على الرغم من ارتباطه بعلم الاجتماع والاقتصاد إلا أن له جوهره في الجغرافيا والتركيز على الفضاء (Space)، خاصة أن غالبية التركيز في مجتمع المعلومات على الشبكات التي تربط المكان وتأثيرها على منظومة الوقت والفضاء. وللدلالة على الارتباط الفضائي بين الناس، فإن نصف بيوت الأمريكان تعمل على الشبكة (Online) وبزيادة (60%) منذ عام 1998م. وفي وزارة الدفاع الأمريكية وحدها (10.000) نظام حاسب منها (2.000) نظام حساس، وهناك (100) مليون آلة مرتبطة بالإنترنت.

7- الاتصالات (Communication)

لقد أدى استخدام الإنترنت على نطاق واسع في الاتصالات والمراسلات الشخصية والرسمية إلى ا لابتعاد عن الرسمنة في التخاطب، والتركيز على المعلومة المرسلة. ولقد نجم عن هذا الاستخدام توفير أطنان من الورق وهذايعني مئات من الأشجار التي يصنع منها الورق، ولم يقف الموضوع عند هذا الحد، فكلفة إيصال الرسالة الورقية باهظة، فلك أن تتخيل كم من الورق تحتاج لكتابة خطاب (مسودة، حتى الوصول إلى الصيغة النهائية) وبعد ذلك يعطى للنسخ ويحتاج الناسخ وقتاً وقد يعيده مرات بفعل الأخطاء ، وبحاجة إلى تغليف وتصدير رسمي إلى أن يصل إلى مكتب البريد وهناك تبدأ عمليات أخرى إلى أن يصل إلى السيارة أو الطائرة أو السفينة التي تنقله إن كان بريداً خارجياً، وتعاد الحلقة بأثر عكسي في بلد الوصول إلى أن يأتيك الرد على تلك الرسالة.

يلاحظ كم من الكلفة الاقتصادية والبشرية قد وضع في عملية بسيطة مثل إرسال رسالة معينة، وعند مقارنة ذلك بالانترنت، فلك أن تعدل رسالتك ما شئت ولن تكلفك شيئاً، كل ذلك من لوحة المفاتيح والشاشة وبعد الانتهاء ما عليك إلا الضغط على مفتاح الإرسال ، ويتلقاها الشخص في الطرف الآخر بمجرد أن يفتح بريده الألكتروني.

ولا يتوقف الأمر على استخدام البريد الإلكتروني وارسال رسالة واحدة لجميع الاصدقاء كبطاقة معايدة، أو رسالة عادية، بل هناك خدمات الفاكسميلي المجانية التي تعطيك رقم فاكسميلي ويمكنك استقبال جميع الفاكسات على بريدك الإلكتروني، ويمكنك استرجاعها من أي مكان من خلال بريدك الإلكتروني. وحتى العزاء يمكنك إرسال بطاقة عزاء وسيأتي اليوم الذي تلغى فيه المراسلات البينية في المؤسسات وحتى مكاتب البريد من الممكن أن تصبح جزءاً من الماضي.

أما مؤتمرات الفيديو والدردشات الصوتية أو المصورة فقد اصبحت شائعة الاستخدام، ولا يتوقف التواصل في جوانب الاتصالات المقبولة اجتماعياً، كالتواصل الاجتماعي بين الافراد في مواضيع شتى. أو كالمساعدة في اختيار الرفيق أو الصديق أو حتى الزوجة من خلال تحديد صفاتك وصفات من ترغب الاقتران به بل تعد ذلك إلى الجنس الفضائي . . .الخ من السلوكيات غير المقبولة اجتماعياً في الكثير من المجتمعات.

8- الأتمتة (التلقائية) (Automation)

لقد حلت التقنيات الحديثة محل الإنسان في كثير من الأعمال، فمنذ دخول الآلة حياة الإنسان كمساعد بدأت تتطور لتحل إحلالاً كلياً محل الإنسان. فمن الطيران والطيار الآلي الذي يقود الطائرة إلى الإنسان الآلي في المختبرات، وفي المصانع، إلى الأتمتة الصناعية بصفة عامة، وإلى المكتب التلقائي، ثم إلى الصراف الآلي للنقود، وإلى الحاسب والمجيب الآلي في المنزل أو العمل . . . إلخ. من هذه التقنيات والتي جميعها تشترك بخاصية التلقائية أو الإحلال محل الإنسان في تنفيذ الأعمال وبطريقة تلقائية.

المركبات الذكية: لقد تأثرت صناعة السيارات بتطورات الحاسب هناك حوالي (500) مليون سيارة في العالم، أي سيارة لكل حوالي (10) أشخاص، وتبلغ مبيعاتها تريلون دولار، وستعتمد صناعة سيارات الغد على الاستشعار عن بعد، ويقول بيل شبراينزر المدير الفني لبرنامج السيارة الذكية في شركة جنرال موتورز «سوف نرى سيارات وطرقات ترى، وتسمع، وتشعر، وتشم، وتتحدث، وتتعرف»، ويمكن للسيارة الذكية أن ترفض تشغيل المحرك عندما تشم رائحة الكحول من السائق، وتعطي موقعها الدقيق إن سرقت، ويمكن من خلال ربط السيارة بالأقمار الاصطناعية أن تنبهك إلى الاختناقات المرورية (كاكو، 2001م). وعرضت قناة الجزيرة مساء يوم (2001/7/4م) برنامجاً عن سيارات المستقبل والمشروع الذي بدأ في فرنسا عن استخدام السيارات الكهربائية التي توجه عن بعد وتخدم التسوق وتجنب المدينة التلوث، وعندما ينتهي الشخص منها تعود أدراجها إلى المكان الذي يراد لها أن تقف فيه، وهي مركبات صغيرة الحجم ومزودة بكاميرات وبخارطة للمدينة تبين موقعك ويتم توجيهها ومراقبتها عن بعد إذا ما تركت وحدها. والجهود مستمرة لتحسين أداء السيارة من حيث كمية استهلاك الوقود وراحة المسافر، والمساعدات المعلوماتية مستمرة، وتستخدم السيارات الحديثة المعالجات الصغرى في الكثير من وظائفها مثل إدارة نظام الطاقة، ونظام الفرامل ضد الإغلاق، والتشخيص أثناء القيادة والتحكم التلقائي في الطقس، والإضاءة عند الحاجة والتكييف التلقائي. ولم تعد هذه الميزات ضرباً من التمنيات ففي سيارة لينكولن كونتيننتال (Lincoln Continental) شملت الخصائص التالية: يسمح نظام موقع قمر صناعي اختياري للسائق ببيان موقع الانقاذ (الإصلاح) عندما تتعطل السيارة، وتستخدم تقنية الأقمار الصناعية في توجيه وإصلاح المركبة. أما نظام مراقب القيادة فيقوم برفع السيارة على محاور عجلاتها، وممتصات الصدمات ويغير نظام عجلة القيادة. ويتحكم مراقب هاتف الخلية في المكالمات . . . إلخ.

ومن النظم المساعدة التي تطورت في هذا المجال نظام يوش ـ بلاوبنكت (Bousch.Blaupunkt) التي تزود السائقين بوسائل سمعية وبصرية، وهناك نظم أخرى تساعد في توجيه السائق من شارع إلى شارع.

ومن المجالات الأخرى ما يسمى بنظام النقل الذكي (Intelligent Transportation System [ITS]) الذي يوفر خدمات عديدة منها :

1- إدارة السفر والنقل (معلومات عن الطريق، توجيه السائق، مراقبة المرور، إدارة الحادثة).

2- إدارة الطلب على السفر (معلومات سابقة عن الرحلات، الطريق، والحجز).
3- عمليات النقل العام (إدارة النقل العام، معلومات الانتقال المتعلقة بالطريق، وبالشخص، أمن السفر).
4- الدفع الإلكتروني (الصراف الآلي).
5- عمليات المركبة التجارية (فحص الأمان على جانب الطريق تلقائيا، التوجيه الآمن أثناء القيادة).
6- إدارة الطوارئ (ابلاغ الطوارئ وأمن الأفراد، إدارة مركبة الطوارئ).
7- نظم الأمن والمراقبة المطورة للمركبة (تجنب التصادم الطولي والجانبي، والتقاطعي، الاستعداد الأمني) (روسنبرج، 2000م).

ثانياً : الخصائص الاجتماعية

1- المعلوماتية الاجتماعية (Social Informatics):

لاتتوقف آثار التقنيات على الجوانب العملية وهي معرفة أثر تصميم المعلومات واستخداماتها ونتائجها وتقنيات الاتصالات(مثل شبكات الحاسبات، والاتصالات العلمية من خلال الدوريات الإلكترونية، واتصال العامة بالانترنت كلها أمثلة للمعلوماتية الاجتماعية) على الحياة الانسانية، وانما تفاعلاتها مع المؤسسات الاجتماعية والسياق الثقافي وما تحدثه فيها من تغيرات في سلوكيات الناس. هناك الكثير من الموضوعات من مثل التغير الاجتماعي الذي تحدثه الإنترنت، أو التجارة الالكترونيه (مثل الامازون Amazon) أو الدفع الإلكتروني (e-Bay) والمخازن الالكترونية، والتعليم الإلكتروني (e-learning) والدوريات العلمية الالكترونية (e-journal) والجامعة الالكترونية(e-University) (Kling, 2000).

2- التغير الاجتماعي (Social Change)

هناك تساؤلات حول نوعية التغيرات الاجتماعية المصاحبة للانتشار والتفجر المعلوماتي، فهل ستحلّ التجارة الإلكترونية (الأمازون وآي بي e-Bay) محل المتاجر المادية؟ وهل سيوفر التعليم عن بعد فرصاً للفقراء للتعليم بكلفة أقل من التعليم العادي؟(Noam, 1995)، وهل سيحلّ التعليم عن بعد مشكلة الاختلاط في الجامعات والجدل القائم حولها في بعض الدول الإسلامية؟ وهل سيحلّ الكتاب الإلكتروني

ج- الموجه الثالثة، عصر التقنيات والمعلومات، والمعرفة، وهي متقدمة أكثر من الموجة الأولى والثانية معاً. في هذا العصر، الناس يتعلمون، ويزداد تعليمهم للحاسب، وهذا يعني وصول أكثر إلى الشبكات الدولية، وفرصاً أكثر للجريمة. ولذا فإن الاهتمام بحماية المعلومات ونظمها ومعلومات الملكية التي يملكها الأفراد، ويخزنونها، أو يرسلونها اهتمام حيوي في عالم المعلومات (Toffler & Toffler, 1994).

في بعض الدول أثرت الموجات الثلاث وبدرجات متباينة في الشدة، والسرعة، والقوة، ومع هذه الموجات ظهر عدم الاستقرار الاجتماعي، والصراع، والتوتر. ويرى توفلر وتوفلر أن التوترات السياسية اليوم ماضية إلى صراع بين الداعين للعصر الصناعي والداعين لعصر المعلومات، إنهما يتصارعان على المستقبل (Kovacich & Boni, 2000).

ويعد المجتمع الصناعي الأساس الذي يتم تطور المجتمع المعلوماتي من خلاله، فالبناء التحتي التقني في المجتمع الصناعي قد ساهم في تطور تقنيات المعلومات الحديثة في المجتمع المعلوماتي، فمثلما دخلت الآلة محل الإنسان في تنفيذ الكثير من المهمات، وخاصة في الزراعة، والتصنيع، والنقل . . . إلخ. فقد حلت المعلومات محل الكثير من الأعمال التقليدية، وحتى أنها حلت محل التفكير، وأصبحت المعلومات رخيصة ومتوفرة وبكميات كبيرة. وكما يقول بلقزيز، في كتابه «نهاية الداعية : الممكن والممتنع في أدوار المثقفين»، أن المثقف سابقاً قد تحددت علاقته بثلاث سُلطات هي سلطة المعرفة، والجمهور (المجتمع)، والحاكم (النظام السياسي)، حيث تشكل السلطة الأولى (المعرفة) المرجع المعرفي، وتشكل الثانية السياق في حين تشكل الثالثة المفارقة والموالاة. ولقد امتدت سطوة السلطان إلى ممالك المثقفين (المعرفة) وحقوقهم (الرأي والتعبير)، ووظائفهم (التوعية والتنوير) مما جعل السلطان في غير حاجة إلى المثقف لتسويغ سلطته المعرفية (بلقزيز، 2000). إلا أن هذ الحاجة لم تعد محصوره على المثقف بل تنوعت مصادرها.

ولقد اتصف المجتمع الصناعي بالتسويق، وتقسيم العمل، أما المجتمع المعلوماتي فقد تركز على الاستخدام المتزايد والمعتمد على المعلومات (الاعتمادية)، وتجدد المصادر المعلوماتية وقوتها مع الاستخدام المتزايد لها، وتغيير البنى الاجتماعية والاقتصادية والسياسية إلى بنى معلوماتية حساسة، والجدول التالي يبين مقارنات لأهم الخصائص للمجتمع الصناعي والمعلوماتي.

جدول رقم (2)

مقارنة خصائص المجتمع الصناعي مع خصائص المجتمع المعلوماتي

الخصائص		المجتمع الصناعي	المجتمع المعلوماتي
الابتكار التقانـي	نواة الوظيفة الأساسية	الماكنة البخارية (القوة) استبدال القوى العضلية بالبخارية والاعتماد عليها	الحاسوب (الذاكرة) السيطرة الذهنية واستخدام القوى الذهنية
	القوة الإنتاجية	قوة الإنتاج المادي	قوة الإنتاج المعلوماتي
البناء الاجتماعي الاقتصادي	الإنتاج المركزي	بضائع وخدمات مفيدة، مصانع حديثة (مكائن وآلات)	معلومات، تقانة معرفية، منفعة معلوماتية (شبكة معلوماتية وبنوك المعلومات)
	السوق	علم جديد، مستعمرات، قوة شرائية استهلاكية	زيادة وتوسع في حدود المعرفة الفضائية
	صناعات قيادية	صناعات معملية (صناعات كيميائية ومكائنية)	صناعات ثقافية (صناعة المعلومات وصناعة المعرفة)
	البناء الصناعي	صناعات أولية وثانوية وثالثوية	مصفوفة البناء الصناعي، انساق صناعية أولية وثانوية وثالثوية ورباعية
	النباء الاقتصادي	اقتصاد سلعي (نظام تقيسم العمل، فصل الإنتاج عن الاستهلاك)	اقتصاد تعاوني (يشترك فيه الإنتاج بالمنفعة)
	أسس اجتماعية اقتصادية	قانون الأسعار	قانون الأهداف

يتبع جدول رقم (2).

	موضوع اجتماعي اقتصادي	مصالح (أهلية وحكومية)	مجتمعات محلية تطوعية
	نسق اجتماعي اقتصادي	ملاك خاصون لرأس المال منافسة حرة، منفعة قصوى	البنية التحتية، أسس التكافل
	شكل المجتمع	مجتمع طبقي (قوة مركزية سيطرة الطبقات)	مجتمع وظيفي (تعدد المراكز، وظيفة مستقلة)
	هدف قومي	الرفاهية القومية	إرضاء قومي
	شكل الحكومة	ديمقراطية برلمانية	ديمقراطية مساهمة، إسهام ديمقراطي
	قوة التغير الاجتماعي	حركات عمالية، اضطرابات	المواطنون، الحركات الشرعيةصدمة مستقبلية
	مشكلات الاجتماعية	حرب فاشية، بطالة	إرهاب، غزو خصوصيات الناس
	مرحلة أكثر تقدما	استهلاك جماهيري عالٍ	إبداعات معرفية جماهيرية
	مستوى القيم	قيم مادية	عالية قيم زمنية (إرضاء حاجات وإشباع الهدف)
	المستوى الاخلاقي	حقوق الأنسان الإساسية	الانتظام الذاتي والإسهام الاجتماعي
	روح العصر	النهضة، التحرر الانساني	العولمة (تكافل وتعاون الإنسان مع الطبيعة).

المصدر : (Youji,1980, pp. 6-7) . موثق في العمر، 2000، ص 34.

3- الشبكات الاجتماعية ـ التقنية (Socio-Technical Networks)

إن العالم يمر بتغير اجتماعي واقتصادي رئيسي، وثورة صناعية ثانية من خلال تكنولوجيا معالجة المعلومات الخاصة بالاتصالات والحاسب (Halton, 1985) . فالحاسبات فائقة السرعة التي تحل العدد الكبير من المسائل الرياضية في أجزاء من الثانية، والستالايت، والألياف الضوئية، والإتصالات، كلها جزء من تدفق المعلومات عبر الطرق الفضائية في البناء التحتي المعلوماتي(Gumahad II, 1996) . وكما يقول بلتون (Pelton) فإن ثورة المعلومات أدت إلى «تغير كل مجالات في عالمنا المعاصر، أساس علاقات القوة يتغير ـ العسكري، والسياسي، والاجتماعي- ولقد تشكل اقتصادنا وأعمالنا»(Pelton, 1992) .

إن تقنيات المعلومات والاتصالات عملياً تمثل شبكات اجتماعية المظهر. ومن الشائع معرفته أن التقنيات ما هي إلا أدوات، والسؤال هوحول أثرها الاجتماعي، وهناك الكثير من الدراسات التي تناولت أثر التقنية في المنظمات الرسمية، وخاصة في الأداء، والتصميم. والبناء . . . إلخ. ولقد أظهرت بعض هذه الدراسات أن الحكومات المحلية والمنظمات الرسمية توظف وتطور هذه الدراسات.

إن الحكومات المحلية والمنظمات الرسمية توظف وتطور نظماً معلوماتية مختلفة اعتماداً على نوع التنظيم الداخلي، ففي بعضها تم تطوير تحكم كبير من قبل الإدارة وتكونت مركزية كبيرة في المنظمات وفي حالات أخرى تكونت لا مركزية. ففي المنظمات الأمريكية قد تم تنظيم الكوادر التقنية بترتيبات مختلفة، وتكوين تقنيات معلومات واتصالات مختلفة، مع تطوير النظم وإعادة البرمجة والعمليات.

لقد تكونت أبنية لتنظيم وتوجيه الاتصالات في تقنيات المعلومات والاتصالات. وبالتالي فإن التغير في نظم المعلومات الراهنة يتطلب الحراك في النظم التنظيمية كاملة، وهذا ما أسماه كلينج ودتون (Kling & Dutton) رزمة الحوسبة المحلية (Local Computing Package)، (Kling & Dutton, 1982) . وتعني رزمة الحوسبة المحلية المزيج من المعدات والناس والأبنية الحكومية وسياسات تقنيات المعلومات والاتصالات. وتتصف هذه الرزمة بـ:

1- أن الناس يلعبون أدوراً متنوعة وعلاقات متنوعة مع بعضهم بعضاً ومع معدات النظام (نظام المعلومات).

2- المعدات (الحاسبات، الشبكات، التوصيلات، معدات الاتصالات).

3- البرمجيات (نظم التشغيل، أدوات النظام، برامج التطبيقات).

4- الأساليب (نماذج وعلم الادارة، التصويت).

5- المصادر الداعمة (التدريب، الدعم، المساعدة).

6- الأبنية المعلوماتية (المحتوى، ومحتوى الخادم، القواعد، الإجراءات). ورزمة الحوسبة المحلية مثال على الشبكات الاجتماعية ـ التقنية (Kling, 2000).

ويمكن المقارنة بين نماذج تقنيات المعلومات والاتصالات والنماذج الفنية ـ الاجتماعية، والجدول التالي يبين ذلك.

جدول رقم (3)

مقارنة بين النماذج القياسية والنماذج الفنية الاجتماعية

النماذج القياسية (الأداة)	النماذج الفنية ـ الاجتماعية
1ـ أداة	1ـ شبكة
2ـ التطبيق مرة واحدة	2ـ التطبيق عملية مستمرة.
3ـ السياسة ليس لها صلة	3ـ السياسة المركزية
4ـ قاعدة البيانات	4ـ المصدر
5ـ العلاقات يسهل إعادة تشكيلها	5ـ العلاقات معقدة، تفاوضية

المصدر : Kiling, 2000, p. 9.

4- الحراك الفضائي (Cyber Mobility)

لقد اصبحت الثقافة والسلوك والجريمة والافقتصاد والسياسة . . . الخ عابرة للحدود الوطنية. توفر خاصية نهاية الحدود الجغرافية بين المجتمعات والدول إمكانية الحراك بلا قيود بين الأفراد والشعوب، مما يتح امكانيات التفاعل الاجتماعي والثقافي عن بُعد بين شعوب العالم. فهذا الحراك جدلي فيه سفر بين المجتمعات ولكن الفرد لم يغادر منزله، وفيه تواصل مع الشعوب عن بعد، فيه تعلم وتعليم عن بعد، فيه عمل وتسوق عن بعد، فيه جريمة عن بعد، فيه إدارة عن بعد. بالانتقال ألى لأفكار والناس والسلع عبر طرق المعلومات أمر متوقع في مجتمع المعلومات. فيمكن أن تحل الإنترنت مشكلة التسوق التقليدي والبحث عن المواقف والتنقل. والحراك لم يتوقف

على الناس والثقافة والمعرفة، بل شمل الجريمة والتي اصبحت تسمى اليوم الجرائم العابرة للحدود الوطنية، والشركات العابرة للحدود الوطنية، والسيطرة على الفضاء الكوني . . الخ.

5- التغير المعلوماتي (Informational change)

استخدم (علي، 2001) مصطلح (الشظايا الثلاثية : النهايات، والمابعديات والمنفيات لوصف البناء الاجتماعي في المجتمع المعلوماتي، والجدول رقم (4) يبين أن المجتمع المعلوماتي هو عصر الاستنساخ اللامتناهي من المعرفة، وعصر الأضداد، والمعرفة قوة، والقوة معرفة، والمعرفة تولد معرفة، والمعلومات اقتصاد، والمعلومات سلاح، والمعلومات هدف للحرب، والمعلومات تفاعل، والمعلومات واقع وتخيل. وهو عصر نهاية الواقع وبداية التخيل، نهاية الجغرافيا والتاريخ والمكان والزمان، والكتاب، والعمل. . وعصر الواقع التخيلي، عصر الفضاء (Cyberspace)، عصرالجريمة عن بعد، عصر حروب الألعاب الإلكترونية، عصر الهواتف بلا أسلاك، ولا أرقام، وعصر المدرسة بلا أسوار، وعصر الشركة المتنقلة بلا تسجيل، عصر ما بعد الصناعة، ومابعد الحداثة، وما بعد المعلومات.

إن عمليات الانتقال البنيوي للمجتمعات (Structural Transformation)، هي قائمة في أغلب المجتمعات وتنتج عن الأثر المدمج للتطور التكنولوجي المبني على تكنولوجيا المعلومات وظهور اقتصاد المعلومات الدولي وعمليات التغير الثقافي والظاهرة بشكل واضح في تغير مكانة الاناث في المجتمع وظهور ا لوعي البيئي. ويعتقد كاستلز (Castells, 1996) أن سقوط الاتحاد السوفيتي ما هو إلا نتيجة عدم قدرته على إدارة التحول إلى مجتمع المعلومات، ويؤكد كاستلز على الصفة الاجتماعية لتكوين المعلومات (Informational Society) والتي هي أبعد من أثر تكنولوجيا المعلومات (Castells, 1996) أن المعلومات عنصر أساسي في عملية انتقال المجتمعات. وتمر المجتمعات كافة بتغيرات هائلة في تغير نمط أبنيتها الاجتماعية والفكرية. ويذكر كليش (2000) أن المدة الزمنية بين كل عصر وعصر قد بدأت تضيق، فقد استغرقت الثورة الصناعية (200) سنة واحتل عصر الكهرباء (40) سنة، ودام العصر الإلكتروني (25) سنة في حين بلغ عصر المعلومات (20) عاماً. ذكر الفن توفلر (Toffler, 1980) في كتابه الموجه الثالثة أن عصر المعلومات هو الموجه الثالثة (Third Wave) ويرى توفلر أن التطور الاجتماعي يتبع سلسلة من الموجات (1) كل واحدة ذات دورة حياة أقل من التي تسبقها ويقول :

الجدول (4)

ثلاثية النهايات والمابعديات ومنفيات «بلا».

نهايات	منفيات	ما بعديات
نهاية المكان	مصانع بلا عمال	ما بعد الصناعة
نهاية المسافة	تعليم بلا معلمين	ما بعد الحداثة
نهاية التاريخ	أفلام بلا ممثلين	ما بعد الفورية
نهاية الجغرافيا	برمجة بلا مبرمجين	ما بعد التيلورية
نهاية الدولة	مركبات بلا سائقين	ما بعد الكينزية
نهاية القومية	مدرسة بلا أسوار	ما بعد الكولونيالية
نهاية المدينة	مجتمع بلا نقد	ما بعد السياسة
نهاية المدرسة	أقلام بلا أحبار	ما بعد الكتابة
نهاية المدرس	هواتف بلا أرقام	ما بعد الرمز
نهاية الكتاب	كتابة بلا أقلام	ما بعد البترول
نهاية المؤلف	مكاتب بلا جدران	ما بعد الإنسانية
نهاية الورق	مكتبات بلا رفوف	ما بعد عصر المعلومات
نهاية الفيزياء	موظفون بلا مكاتب	
نهاية المكتبة	رواية بلا نهاية	
نهاية المتحف	سياسة بلا نواب	
نهاية الميتافيزيقا	ترحال بلا انتقال	
نهاية الأيديولوجيا	حضور بلا وجود	
نهاية الأضداد	جيرة بلا قرب	
نهاية العمل	جنس بلا رفقة	
نهاية الطبقة المتوسطة		
نهاية الوسطاء		
نهاية الذاكرة		

المصدر : علي، 2001، ص 15 ..

«إن السباق البشري قد مر في موجتين عظيمتين من التغير كل واحدة تطمس (Obliterating) الحضارة والثقافة السابقة، وتحل محلها بطرق حياة لم تكن في اعتقاد

(Inconceivable) أولئك الذين أتوا قبلها. الموجة الأولى من التغير (الثورة الزراعية) وقد احتاجت لمئات السنين لكي تظهر نتائجها. الموجة الثانية (ظهور الحضارة الصناعية)، وقد احتاجت (300) سنة. أما تاريخ اليوم فأكثر سرعة ومن المحتمل أن الموجة الثالثة قريبة الوصول وستكتمل خلال عدة عقود قليلة» (Tofler, 1980, p. 26).

6- التفاعل الفضائي (Cyber Interaction)

إن تقليد السلوك البشري والحياة البشرية من الموضوعات التي أثارت اهتمام الإنسان من قديم الزمان، وتتلخص هذه الفكرة بقول جورج برنارد شو (1856-1950) «يرى بعض الناس الأشياء كما تكون، ويسألون لماذا، ويحلم بعضهم الآخر بأشياء لم تحدث على الإطلاق ويسألون لم لا؟» (Harris, 1995). ولقد أصبح التخيل من المواضيع المرغوبة والتي وصلت إلى درجة يصعب الفصل فيها بين الواقع والخيال، لا بل سمي الواقع التخيلي أو الافتراضي إشارة إلى هذا النوع من الواقع. فظهرت الأفلام مثل حرب النجوم (Star Wars) والتي لاقت انتشاراً.

ولقد ساعدت الإنترنت في توسيع نطاق التخيلية عند الإنسان من الموسيقى إلى الفنون، إلى السياحة إلى السفر، إلى تصفح المكتبات والكتب والدوريات العلمية، إلى الشوارع والطرق وحتى إلى غرف النوم في الفنادق وحمامات السباحة، إلى حالة الطقس، كل ذلك يُمكن الشخص من الإطلاع واتخاذ القرار المناسب أو الاستفادة أو طلب الخدمة المناسبة. ولم تتوقف التخيلية عند هذا الحد، بل شملت الآلات، وخاصة الإنسان الآلي، وموضوع الذكاء الاصطناعي، وإيجاد آلات تفكر بدلاً عن الإنسان، وتقوم بعمل بدلاً منه، وتتخذ القرارات، لا بل أصبحت الآلة شاعراً ولاعباً ومتحدياً للإنسان في كل شيء.

إن ربط الملايين من البشر والمنظمات عبر ملايين من شبكات الحاسب يحول هذه الشبكة الإلكترونية إلى شبكة اجتماعية كونية (Global Social network). هؤلاء الأفراد بعضهم لم يسبق له أن رأى أو سمع أو التقى ببعضهم الآخر، حتى إن بعضهم لا يتكلم لغة الآخر، ولكن الشبكة كأداة جعلت ذلك ممكناً. ويرى متشل (Mitchell,1995) أن فكرة الطريق السريع للمعلومات، والطريق فائق السرعة قد أسس

1- الموجة هنا استعارة لحركة التنمية الشاملة والتغير الاجتماعي وتكوين حقبة زمنية ما.

على فكرة اجتماعية مفادها أن المجتمع المعلوماتي قائم على التبادل المعلوماتي (Information exchange)، وكما أن العلاقات الإنسانية تبادلية فإن أساس هذا التبادل الآن هو المعلومات، وليس بناءً على المكان (place). لقد أدت الإنترنت إلى تغير في بعض المجتمعات (خاصة الغربية) من السياق في المكان العام إلى السياق في المكان الخاص، وطورت أعرافاً خاصة بها، ولقد دعمت الإنترنت من خلال الربط الإلكتروني تحويل الحياة في المنزل والعمل إلى أنماط جديدة مغايرة في تراكيبها لما هو سائد في المجتمعات الواقعية.

تشكل شبكة الإنترنت أداة ربط بين الأفراد تمكن من التواصل المتبادل والمتعدد حجماً وثقافة ولغة ومكاناً وزماناً، وتمثل المعلومة (المتخصصة أو العادية أو الترفيهية) أساس التبادل في هذه العلاقات، هل يبقى الأفراد في هذه العلاقات أم ينسحبوا منها؟ يعتمد ذلك على عوامل.

هنالك من يرى أن العلاقات على الشبكة تتسم بالسطحية والضعف وقد لا ترقى ألى أن تصل إلى مستوى العلاقات الطبيعية في المجتمع المحلي، إلا أن هذه العلاقات تتسم أيضاً باستكمال المعلومات، وتوفر الدعم الاجتماعي والعاطفي والمساعدة المادية والفنية والإحساس بالأهمية والإحساس بالوجود، حيث يمكن للأفراد أن يتسوقوا وهم مستلقون في غرف نومهم ويجدون المصادر الاجتماعية أكثر سهولة مما هو في المواقف الحياتية الاعتيادية، ويمكنهم التسوق بأمان وراحة مساوية لما هو متوافر في منازلهم أو مكاتبهم. بالإضافة إلى البحث والتنقل (التخيلي) أو السفر دون استثمار يذكر في المال أو الطاقة. ويؤدي هذا التفاعل والذي ربما يستمر لفترة بسيطة من الزمن إلى تكوين مجتمعات منظمة بسبب المصالح المشتركة وليس بفعل عامل المكان أو القرابة (Mitchell,1995).

ويرى سلوكا (Slouka,1995) أن العلاقات على الشبكة ضيقة وينقصها النوعية، والخوف من أن سهولة استخدام الشبكة قد أدت بالناس غير المؤهلين من تقديم معلومات مضللة كما هو الحال عندما يقوم الناس العاديون بتقديم نصائح طبية أو نصائح تتعلق بأنواع السيارات . . . إلخ. ويبين رينجولد (Rheingold, 1993) أن المستخدمين يحصلون على معلومات من الشبكة من خلال روابط ضعيفة بينهم، ويبين كيف أن تراكم التفاعلات البسيطة والأفعال بسبب الحاجة للمساعدة يمكن أن يحافظ على المجتمع المتكون على الشبكة والمجتمع الفعلي للأفراد، حيث إن كل فعل ينظر

إليه من خلال الجماعة كلها ويساعد في تكوين الانتماء إلى التبادلية المعممة (Generalized reciprocity) والمساعدة المتبادلة (Mutual aid)، وذلك لأن المساعدة على الشبكة تعزز إيجابياً من قبل أعضائها "الفرد الذي أساعده، قد لا يساعدني إطلاقاً، ولكن ربما شخص آخر يستيطع ذلك"، وهذه العملية كما أسماها ميد وكيلي أخذ دور الآخرين (Taking the role of others)، حيث أن كل مستخدم يضع نفسه مكان الآخرين ويتوقع أنه لو كان مكانهم لقدم المساعدة، وبذلك فالفرد يستجيب لتوقعات الآخرين فيما يخص سلوكه الشخصي.

وترى رينجولد (Rhengold, 1993) وتيركل (Turkle, 1995) أن عمليات تقديم الدعم والمساعدة والمعلومات على الشبكة يمكن أن تكون طرقاً للتعبير عن هوية الشخص خاصة إذا أدرك أن الخبرة الفنية أو السلوك التدعيمي جزء من الهوية الذاتية. أن التفاعل على الشبكة يمكن أن يكون ثقافة في ذاته.

إن قلة المؤشرات (Clues) الفيزيقية والاجتماعية على الشبكة تجعل من الصعب اكتشاف خصائص المشاركين الاجتماعية والفيزيقية. لقد أبدى ستول (Stoll, 1995) وسلوكا (Slouka, 1995) قلقهما بخصوص ضيق الاتصالات عبر الحاسب والتي قد تعمل ضد المحافظة على علاقات طبيعية قوية، وشكا بأن هذه العلاقات يمكن أن تكون قوية دون مؤشرات فيزيقية واجتماعية ودون تفاعل فوري وجهاً لوجه. ويقول ستول في هذا المجال «إن الاتصالات الإلتكرونية تمثل اتصالاً خيالياً آنياً يؤدي إلى تكوين الاحساس بالعاطفة دون استثمار عاطفي يؤدي إلى علاقات صداقة قوية» (Stolle, 1995, p. 24) .

وتشجع الشبكة المشاركة المتعددة أو الجزئية، حيث يشترك الأفراد في نقاش متعدد من قبل جماعات الأخبار أو إرسال الرسائل . . . إلخ. ولكن هناك تبايناً في مقدار انغماس مشاركتهم. إن الروابط التي تتطور على الشبكة لا تختلف كثيراً عن الروابط التي تنشأ في الحياة الواقعية وهي أنواع منها للتسلية ومنها المتخصصة، وهي متباينة في قوتها، ونوعية اتصال الأفراد متباين كذلك فمنهم المنغمس جداً في اتصال متكرر ومنهم قليل الاتصال.

ويثير ستول وسلوكا مخاوف أخرى مفادها أن الانغماس الكبير على الشبكة كمجتمع تخيلي سيكون على حساب الانغماس في العلاقات الاجتماعية في الحياة

الواقعية في المجتمع المحلي. وهذا الخوف ينظر إلى هذه المعادلة كمحصلة صفرية (Zero sum game) وهذا يعني أنه إذا أمضى الفرد وقتاً أكثر على الشبكة فسيكون على حساب الوقت الفعلي الذي يقضيه في المجتمع المحلي، والمنطق الرافض لهذه الفكرة مبني على أن روابط الإنسان الحالية الفعلية هي بالمعدل (10-20) رابطة علاقات في المجتمع الفعلي، وأنه حتى في الريف والذي يمتاز بكثرة الروابط فلم تعد العلاقات وجها لوجه سائدة فيه خاصة مع دخول التلفون والجوال والفضائيات في المنازل.

إن العلاقات هي الشيء المهم وليس الوسيلة المستخدمة في تكوينها (Slouka, 1995) (Stolle, 1995). لقد طورت التفاعلات على الشبكة أعرافاً وبنىً اجتماعية وهي ليست تقليداً للحياة الواقعية. إن البناء الهيكلي للشبكة يدعم المحافظة على العديد من الروابط في المجتمع المحلي. إن بناء الشبكة وعدم كلفة المسافة بين الأفراد وتكون روابط روحية أكثر من الهاتف أو السيارة أو الطائرة وأن طبيعة الإنترنت (Asyrchronous nature) تشجع الاتصال في أوقات واحدة لمناطق ذات أوقات مختلفة، إنها تجعل من الإنسان أكثر "عولمة". إن الوصل الإلكتروني يقلل أهمية المحلية (Locality) للمجتمع المحلي.

وكما يصف متشل (Mitchell) الإنترنت بأن «لوحة المفاتيح هي مقهاي» (Mitchell, 1995, p. 7) لأن الفرد قادر على التواصل مع الآخرين والرد على رسائلهم وتكوين صداقات جديدة وهو لم يغادر غرفة نومه، حتى إنه يمكنه المشاركة بمؤتمر أو إدارة أعماله كذلك دون مغادرة منزله. إن التواصل عبر الشبكة يعزز قدرة الأفراد على الحركة بين الروابط (Ties) والشبكات الاجتماعية وهي تزيد النزعة في الانتقال إلى التعامل مع المجتمع المحلي خارج المكان العام وتساهم في تكامل النظم الاجتماعية ودعم الروابط التي تتقاطع مع جماعات المصالح والمحليات والمنظمات والدول.

7- التفاعل عن بعد (Remot Interaction)

لم توفر تقنيات عصر المعلومات من معدات وبرمجيات خاصية التخيلية للمجتمع وإنما قربت المسافات واختزلتها إلى حد إلغائها من الناحية العملية، فأصبحت المسافة بين الشاشة والعين هي المسافة بين الفرد وأي شيء يتفاعل معه (عمل إداري أو تواصل أو بحث . . إلخ) يضاف إلى ذلك التفاعل عن بعد على الشبكة. فلم يعد مهماً أن نلتقي ونسافر لكي نعقد الصفقات أولشراء السلع وإنما يمكن إجراء كافة النشاطات الإنسانية من خلال الحاسب والإنترنت والشاشة. وفي مجال العلاقات الانسانية فقد

انتشر استخدام الدردشات (Chatting) بين الأصدقاء والغرباء وبين أفراد الأسرة الواحدة، وتطور ذلك من الدردشات المكتوبة (النص فقط) إلى الصوت إلى الصوت والصورة (فيديو) الى المؤتمرات التي تجمع أكثر من شخصين ومن أمكنة مختلفة. لا بل أصبحت شركات متخصصة في إجراء المؤتمرات الحية (فيديو) بين الأفراد من مثل المؤتمرات والمناقشات العلمية. وفي المجال الأمني لم يعد السارق بحاجة إلى أن يذهب ليسطو على بنك ما أو سلعة، فاعتراض بطاقة الائمان وهي في طريقها إلى البائع أو تحويل الحسابات من مكان لآخر أو سرقة المعلومات ونقلها يمكن أن تحدث والفاعل الحقيقي في مكانه والهدف أو المادة المسروقة في مكان آخر. ويمكن القول إن عمليات مثل التسوق عن بعد أو الاستشعار عن بعد، وعقد المؤتمرات عن بعد، والتعليم عن بعد، والإنتاج عن بعد، وتشخيص الأمراض عن بعد وإجراء العلميات الجراجية عن بعد ـ قد أصبحت واقعية في مجتمع تخيلي.

8-المشكلات الاجتماعية المعلوماتية

كثيرة تلك الموضوعات التي ظهرت في مجتمع المعلومات وكثيرة هي المشكلات المصاحبة لها، فموضوع الإنسان الآلي والأتمة والاتصالات والحوالات الإلكترونية والإنترنت والذكاء الصناعي، والبريد الإلكتروني .. إلخ. كلها مواضيع جديدة ظهرت في مجتمع المعلومات.

إن هذه المواضيع ذات تطبيقات مفيدة للإنسان ولكن صاحبها مشكلات اجتماعية أخرى غاية في الأهمية، ففي مجال العمل ظهرت البطالة، وجرائم الحاسب، وخرق الخصوصية، وضياع المسؤولية، وتهديد حرية التفكير، ومشكلات الملكية الفكرية، ومركزية السلطة والمراقبة، هذا بالإضافة إلى مشكلات تتعلق بترويج الصور والأفلام، والخيالات والأصوات، والمواقع الإباحية والجنسية، والاتجار بصور الأطفال لغايات الجنس، والمضايقة على الشبكة، والتعقب الشخصي وخاصة للمشاهير،وظهور مصطلحات جديدة مثل الجنس الفضائي (cybersex)والاغتصاب الفضائي(cyberrape).. إلخ (البداينة، 1997 أ). والجدول التالي يبين العلاقة بين هذه الموضوعات والمشكلات المصاحبة لها.

جدول رقم (5)
الموضوعات التقنية والمشكلات الاجتماعية

المشكلات / الموضوعات	العمل	الصحة	الخصوصية	مركزية السلطة	المسؤولية	مجتمع المعلومات	كرامة الانسان	التحصين والأخلاق	المصالح الوطنية	الأفضلية	حرية التعبير	الملكية الفكرية
الإنسان الآلي	•	•	•				•		•	•		
أتمتة المكتب	•	•	•	•	•	•	•	•		•		
الاتصالات	•			•		•		•	•		•	
الحوالات المالية			•									
الإلكترونية	•			•	•			•				
المعالجات الصغرى	•	•	•			•		•		•	•	•
البريد الإلكتروني	•			•		•			•			
الذكاء الصناعي	•		•			•	•		•			
الواقع التخيلي		•				•	•					
الإنترنت	•			•	•	•		•	•		•	•

المصدر : روسينبرج، 2000، ص 55.

ومن القصص المشهورة في هذا المجال قصة جل بيكر (Baker) طالب بجامعة ميتشيغان (UM) حيث كان يرسل قصصاً إخبارية على المجموعة (Usenet) تحت مسمى (alt.sex.stories) وهي قصص ذات طبيعة إباحية ومثيرة، وتشير إحدى القصص إلى امرأة يعرفها بيكر، مما استرعى انتباه الإدرايين في الجامعة، حيث تم تفتيش غرفة بيكر ورقم حسابه وبتصريح منه شخصياً، تبين أنه كان يتصل من خلال البريد الإلكتروني بشخص في كندا هو جوندا (Gonda)، وكانا يتناقشان في احتمالية

خطف شخص بغرض التعذيب بما يتماشى مع ما كان موصوفاً في القصص. وانتهى الأمر بفصل بيكر من الجامعة وأدانت الـ(FBI) له بالتهديد بخطف شخص. ولقد أثارت هذه الحادثة الموضوعات التالية:

1- خصوصية الضحية. هل من حق بيكر استخدام اسم الضحية في حديثه الحر؟ دون معرفتها وموافقتها؟

2- التهديدات، هل مثلت هذه الحادثة تهديداً للضحية؟ أم يمكن أن تعد مجرد خيالات بين اثنين.

3- العلاج. هل يمكن أن يعد تصرف بيكر نوعاً من العلاج الذي كان يقوم به لصرف الغضب كما قال.

4- الدور. هل كان بيكر يقوم بدور ويصف فيه سلوكه أم سلوك الآخرين، وبالتالي لا تخرج هذه الحادثة عن بعض الدور التخيلي.

5- الرذيلة. هل يمكن أن تعد قصص بيكر فحشاً أم أنها محمية بالحديث الحر؟

6- الإدانة: هل يعد بيكر مداناً للجامعة وهل يعامل كمجرم؟ بناءً على ما كتبه.

7- الإنترنت: هل خرق بيكر أو أساء استخدام الإنترنت؟

8- نمط الفاحشة: هل قصص بيكر مخالفة للانترنت.

وهذه القضايا والأسئلة لم تعد تخص حادثة بيكر ولكنها مدار حديث وجدال على الكثير من المواضيع والقضايا على الإنترنت.

دراسة رايم (,Rimm)من جامعة كارينجي ميلون (.Carnegie Mellon Un) في بتسبرج بولاية بنسلفانيا حول الرذيلة على الشبكة. حجمها وزبائنها، ولقد ظهرت هذه الدراسة في مجلة أكاديمية هي مجلة القانون بجامعة جورج تاون وفي مجالة التايمز (Rimm, 1995; Elmer-Dewitt, 1995)، وفيما يلي ملخص لأهم نتائج الدراسة:

1- وجود كم هائل من المواد الإباحية تم مسح (917310) صورة وصف وقصة قصيرة ولقطة فيلم جنسية فاضحة وكان (83.5%) من صور المجموعات الإخبارية المخزنة صوراً إباحية.

2- أنها واسعة الانتشار، حيث تعد تجارة الجنس التخيلي تجارة رائجة على الانترنت.

3- أنها تجارة مربحة وبمبلغ (10-30 دولار) اشتراك شهرياً، ولأكبرخمسة منها نظم لوحات نشر (BBS) تزيد عائداتها عن 1 مليون دولار.

4- غالبية الزبائن من الذكور (98.9%).

قدم روسينبرج (Rosenberg) ست قواعد لتنظيم الحديث الحر، وذلك على النحو التالي:

1- عدم معاملة الوسط الإلكتروني بطريقة مختلفة عن الوسط المطبوع، أو النشر التقليدي.

2- تشجيع استخدام الإجراءات المانعة للمضايقة بدل مراقبة المادة الهجومية على الشبكة.

3- الحذر في المسؤولية (الاستخدام وسوء الاستخدام) في التسهيلات.

4- الثقة بالآخرين وتعليمهم المسؤولية.

5- تتكاثر الموضوعات أكبر من قدرة المنظمات على المراقبة.

6- لا تتأثر الرسائل الهجومية من مكاسب عبر الشبكات الإلكترونية (Rosenberg, 1993).

ومع سن تشريعات خاصة في الولايات المتحدة الامريكية تجيز للأجهزة الأمنية مراقبة البريد الإلكتروني وخرق خصوصية المواطن، فقد اصبحت مشكلة تتعلق بالموازنة بين الحرية والأمن. فهل يضحي المواطن بحريته من أجل أمنه؟

ثالثاً : الخصائص الثقافية

1-الثقافة الكونية (Global Culture)

في مجتمع المعلومات حيث امكانية توحد المكان وذوبان الفوارق بين الدول، قد تتشكل ثقافة كونية ناتجة عن الانتشار الثقافي لكل مجتمع، والتثاقف المتبادل بين الثقافات لتتشكل في النهاية ثقافة اجتماعية عالمية. وعلى الرغم من أن هذه الثقافة قد أصبحت مظاهر تشكلها واضحة بفعل التقارب الحضاري بين المجتمعات، فقد أصبحت ترى الملابس (والموضة) تنتشر في كل مكان، وترى أنواع الطعام الشرقي منها والغربي ومع مرور الزمن قد لا نجد مثل هذه التسميات (طعام صيني، أو عربي، أو... إلخ) فالمعايير الدولية تشكل أساس لهذه الثقافة، فعدم الاعتداء وحل

الخلافات بالطرق السلمية ووقوف المجتمع الدولي ضد المعتدي، ومنظمات الأمم المتحدة هي بدايات لهذا التشكل.

وتُعد الإنترنت من أهم الوسائل التقنية التي ساهمت في تكوين ثقافة عالمية من خلال إمكانية التواصل العالمي بين الأفراد، والفرص المتاحة للتعرف على الثقافات الاجتماعية الأخرى. إن توافر المعلومات بشكل كبير، وامكانية استرجاعها بفترة زمنية قصيرة، والاطلاع عليها جعل إمكانيات الفهم الثقافي العالمي أكبر من أي وقت سبق. إن امتياز شبكات الإنترنت بامكانية التواصل ليس المكتوب فقط وإنما المشاهد، والمسموع، والتواصل بطريقة تفاعلية (Interactive) مكن ليس من التقارب الثقافي وإنما من التواصل والتقارب المكاني بين الأفراد رغم اختلاف الزمن والمكان والثقافة. يدعم هذا نظام الشبكة الذي أصبح يحمل إمكانيات الترجمة والكتابة بلغات متعددة.

إن الربط الإلكتروني العالمي قد قلل احتمالية الأفراد في التمركز العرقي، والذي يعني اعتماد الفرد على معاييره الاجتماعية في الحكم على سلوكيات الأفراد في الثقافات الأخرى. إن تقليل هذه الاحتمالية ناتج عن التقارب الثقافي بين الأفراد في العالم، ومعرفتهم بخصوصيات الثقافات الأخرى واحترامها.

2- العولمة (Globalization)

العولمة ليست ظاهرة جديدة في جوهرها بمعنى الانسياب الاقتصادي والتجاري والثقافي بين الدول والمجتمعات. فانتشار الثقافات بين المجتمعات في اللغة، والسلوك، والقيم، وعادات اللباس والطعام من الامثلة الشائعة في هذا المجال. وكذلك الحال في العلوم، فانتقال العلم بين الشعوب وتأثرها المتبادل ظاهرة معروفة عبر التاريخ. فعلماء المسلمين استفادوا من علماء في ثقافات أخرى، فابن سينا قد تأثر بأبو قراط، وابن رشد بأرسطو. إن التطورات في وسائل المواصلات والاتصالات وشبكات الحاسب ذات تأثير رئيسي في كافة الذخائر التقنية والمعنوية والثقافية بين الشعوب والمجتمعات، ولايتوقف الأمر على عولمة التكنولوجيا، والحاسب، والثقافة والطعام الصيني وإنما رافقها عولمة في ربط الدول النامية مع الدول المتقدمة أدى إلى حراك فعلي والكتروني للمجتمعات خاصة بين المجتمعات النامية والصناعية وما بعد الصناعية، مما أدى إلى عولمة السوق الدولية، فديون المجتمعات النامية وزيادة الفوارق في الدخل بين الدول أسهمت في رفع الجريمة الدولية وخاصة المخدرات، كل هذه

الظروف جعلت من الجريمة عابرة (Transntional) للحدود الوطنية، ودولية (International) ومتداخلة (Interdependence) بين الدول.

تعد العولمة أوضح خصائص المجتمع المعلوماتي، فبفعل الشبكات والاتصال الفعال بين المجتمعات، غدا المجتمع الدولي كينونة واحدة، فتكونت الشركات متعددة الجنسيات واندمجت كبرى الشركات لتكون وحدة واحدة مسيطرة في مجال أعمالها من مثل اندماج شركة مرسيدس بنز الألمانية وشركة كريسللر الأمريكية. فالعولمة لم تقتصر فقط على العولمة الاقتصادية التي تنطلق من أن السوق الاقتصادية العالمية واحدة وهي ملك للجميع ولهم الحق في التنافس فيها وهذا ما أدى إلى وضع اتفاقية (الجات).

عولمة الأمن: لم يعد تهديد الأمن مشكلة وطنية أو اقليمية بل غدا مشكلة عالمية، ولا غرابة في أن نرى الإهتمام العالمي من كافة الدول الصناعية والنامية بمواضيع تهددهم جميعاً كتلوث الأرض، والأوزون، والجريمة، والسلام، والأمن العالمي. وفي المجتمع المعلوماتي فإن إستتباب الأمن ليس قضية محلية أو وطنية وإنما عالمية، فالذي يخرق عرفاً أو قانون لا تتوقف آثاره عند الحيز المكاني الضيق الذي يعيش فيه، ناهيك عن أن طبيعة السلوكيات الإجرامية ستكون مختلفة في طبيعتها وبالتالي فإن عولمة الانحراف سمة من سمات المجتمع المعلوماتي.

وبما أن المجتمع الكوني في عصر المعلومات مجتمع كلي فإن محصنات الأمن ستكون محط اهتمام الجميع وأن تهديد الاستقرار العالمي ذو تأثيرات سلبية على الجميع. وفي المجتمع المعلوماتي قد لا يكون تحكم الدولة بحدودها أمراً ممكناً بالوسائل التقليدية. ففي وجود أقمار التجسس والأطباق الفضائية. لم تعد السيادة الوطنية ممكنة.

إن وجود أعراف إنسانية ذات صبغة عالمية تتعلق بالأمانة والصدق والعدالة، والمساواة، ومحاربة المخدرات . . .الخ، مما يجعل خرقها يشكل انحرافاً وجريمة، وكذلك الحال فإن كثيراً من السلوكيات والنواهي مشتركة بين الأديان السماوية، وهناك أعراف اجتماعية ذات انتشار عالمي مثل معاشرة المحارم من الإناث. . . الخ هذه العوامل جعلت من الجريمة ذات صفات عالمية. وعالمية الجريمة (وجود قواسم مشتركة

لها) تسهل عولمتها (انسيابها بين المجتمعات). لقد غدا الأمن مطلباً عالمياً كونياً، وبالتالي من المتوقع أن تتضافر الجهود لمكافحة مهدداته.

عولمة الجريمة: إن انتقال التقنيات إلى جماعات الجريمة أصبح من الأمور السهلة والميسرة، وبالتالي فإن استثمار هذه التقنيات في ارتكاب الجرائم من الأمور الميسرة. إن نقل تراكيب السلاح النووي والكيميائي والنووي لم يعد يتطلب عمليات استخبارية وسرية كبيرة ويمكن نقل ملفات البيانات التي تشمل كافة المعلومات بكل سهولة.

إن زيادة الاعتماد على التعاون الدولي في مكافحة الجريمة وخاصة الإرهاب والمخدرات والدعارة، وغيرها من الجرائم أصبح من الدلائل الواضحة على تحول الجرائم من النمط الوطني والمحلي إلى جرائم عابرة للحدود الوطنية. ومع ظهور أنواع حديثة من الجرائم تعتمد في تنفيذها على التقنيات المتاحة في هذا العصر، جعل غالبية الجرائم تنزع إلى كونها إلكترونية وفضائية. فلم يعد السارق بحاجة إلى اقتحام بنك لسرقته، أو سرقة أو نشل المارة في شارع مزدحم، وإنما يمكن الدخول إلى أرقام حسابات متفرقة ومن ثم تجميعها في مكان ما. المجرم في المجتمع المعلوماتي يمكن أن يرتكب الجريمة من مكان ويحولها إلى مكان آخر، وينتقل من مكان لآخر بسهولة. كما يمكن استخدام التقنيات المتاحة "للاغتيال النفسي"، و"التشهير" بوضع معلومات فاضحة وغير صحيحة عن الأفراد المهمين، أو وضع معلومات تتعلق بخصوصيتهم على الشبكة (البداينة، 2000).

عولمة القانون : لقد ظهرت الكثير من الموضوعات القانونية المرتبطة بزيادة ترابط العالم، فظهرت موضوعات الإزعاج والتشهير والمواد المعادية للعرق والدين، والكل يتذكر المحاكمة الشهيرة لسيمبسون (O.J. Simpson) حيث كانت المعلومات متاحة على الإنترنت لأقرب دقيقة، وكانت كل الجلسات متاحة على الإنترنت لأقرب دقيقة، وكانت كل الجلسات متاحة للمتابعة عن بعد. كل يوم كان برشويز (Pershowist) يشارك (محامي الدفاع) إلكترونياً من مكتبه في لوس انجلس أو من منزله في ماساتشوسس. لقد نجم عن تطبيقات الحاسب في هذا المجال حقول جديدة للمحامين مثل التقاضي في مواضيع أخطاء البرمجيات، أو المعدات بالإضافة للجرائم المتصلة باستخدام الحاسب عامة، وسوء استخدام الحاسب وفيروسات الحاسب وديدانه، والتعديات على الإنترنت ومهاجمة المواقع الإلكترونية والتجسس الإلكتروني (روسينبرج، 2000).

ولم تتوقف العولمة عند الجريمة فقط، بل تعولم القانون، فمع عولمة الاقتصاد والاتفاقيات الدولية التي تجعل من العالم سوقاً اقتصادية واحدة يحكمها التنافس، ويلعب الاقتصاد الإلكتروني فيها دوراً كبيراً، فإن النزعة قد أصبحت نحو تعديل القوانين المحلية وتعديلها لتناسب مع القانون الدولي وبالتالي عولمتها.

ولم يتوقف الأمر على مكافحة الجريمة، بل تعدى ذلك إلى فض النزاعات، وتحكيم القانون الدولي حتى في محاكمة زعماء الدول الذين يخرجون على الامتثال الدولي، والقانون الدولي، وقد أصبح دور الأمم المتحدة متزايداً بشكل أكبر مما سبق.

ويتوقع أن يشهد هذا العصر مزيداً من التحول نحو القانون الدولي في تسليم المجرمين ومكافحة الجريمة والإرهاب، والمخدرات، وحتى في حل النزاعات السياسية بالمفاوضات، وليس بالحروب التقليدية.

3- التعليم الالكتروني (e- Learning)

إن التغيرات التقنية الكبيرة التي أصابت العالم لم تقف تأثيراتها عند التجارة والإعلام والثقافة بل شملت جميع النظم الاجتماعية بما فيها التعليم، وهناك مؤشرات على عولمة التعليم، وانبعاث الجامعة الفضائية (Cyber University)، أو الجامعة الإلكترونية (e-university) وبدأ طرح شعارات جديدة للتعليم كشعار التعليم لجميع العالم (all the world) وتكون فرق البحث الدولية، والربط الإلكتروني لمكتبات العالم، وكذلك أبحاث الموسوعة العالمية، والعقل الدولي والطالب العالمي والجامعة العالمية والتعليم مدى الحياة (Rossman, 1992). التعليم هو الاستثمار الأفضل في المجتمع المعلوماتي (Gates; Myhrvold & Rinearson, 1995) حيث الحوارات بين الطلبة عبر المحيطات بلا حدود جغرافية أو سياسية، وسيصبح التعليم مستمراً على مدى الحياة، وغير محد بمُدرس أو بعُمر أو منهاج، وسيركز على الانفتاح والاستمرار والذاتية وسيكون عن بعد وبلا مدارس. والتعليم حجر الزاوية في المرحلة القادمة ويشكل قضية أمن قومي ومستقبل أمة، ودعمه دعم للأمن القومي وهو مفتاح الأمن والعامل الرئيسي في محاربة الفقر (يماني، 1998). ويشكل الانفتاح من العزلة المصانة إلى الانفتاح اللامحدود (ناظر، 1998). المجتمع المعلوماتي سيغير حواجز الزمان والمكان لإنتاج حضارة وطنية. كما يؤدي إلى عولمة المعرفة. وسيرتبط العالم بما أسماه جتيس

بطريق المعلومات السريع والفائق السرعة مثلما هي المدن مرتبطة بالطرق السريعة. إن أي تحسن في التعليم سيؤدي إلى جعل الفرص متساوية أمام الناس. إن كل هذه التغيرات قد أدت إلى ظهور البنية التحتية المعلوماتية العالمية (Global information infrastructure) مما جعل أمن التعليم مسؤولية عالمية لحماية هذه البنية والتي تتم عليها كافة الاتصالات والتفاعلات. وأضحى الوعي بأمن المعلومات وسلامتها مطلباً دولياً، وشمل ذلك تأمين موثوقية الاتصالات، وأمن الحاسبات والشبكات، والأمن الفيزيقي ... الخ. وبدأ التركيز على عمليات الأمن والتحكم ووضع سياسات أمن المعلومات وإجراء دراسات تقدير الخطورة، وإدماج أمن المعلومات في عمليات البناء الأولية في التصحيح والفحص والمراجعة. ولكن إجراءات الحماية والأمن تواجه تحدياً في الموافقة بين الحرية وإجراءات الأمن، والسؤال هو إلى أي درجة يضحي الناس بحرياتهم وخصوصياتهم مقابل الحماية والأمن؟. ولقد بدأت مناقشة مواضيع أخلاقية برزت مع دخول المجتمعات لعصر المعلومات منها: احترام الملكية، واحترام الحدود الخصوصية، واحترام الآخرين، واحترام المؤسسات، واحترام الذات. حيث إن هذه المواضيع الأخلاقية تتأثر بالسلوكيات على الشبكة والتي بدورها يزيدها ضعف التغذية الراجعة الفعالة، ويقف الخوف من خطورة الكشف والعقاب والدخول في بيئة جديدة وقواعد جديدة وإدراك الظلم الاجتماعي والفساد (Willard, 1998).

ولقد أدت التعديات التي منيت بها شبكات المعلومات والإنترنت والحاسبات بإثارة مواضيع تتعلق بأمن المعلومات منها:

أ- الحماية والقدرة على حماية المعلومات من السرقة، أو التدمير، أو التعديل من قبل مستخدمين غير شرعيين.

ب- ضبط الدخول (Access of Control) وهذا يشمل تحديد الأشخاص المسموح لهم بالدخول إلى شبكات المعلومات وضبط هذه العملية بحيث لا يسمح للآخرين دخول الشبكات.

ج- الهوية (Authentication) وهي عملية التأكد من الهوية أو شرعية الدخول والتأكد من الشخص الذي دخل هو ذات الشخص الذي قال إنه هو.

د- المسؤولية (Accountability) وهي المقدرة على منع الأطراف المتصلة من نكران إرسالها واستقبالها للرسائل التي أرسلتها أو نكران انغماسها في نشاطات على الشبكة.

هـ- الموثوقية (Confidentality) وهي القدرة على حصر الدخول الشرعي وحماية المعلومات التي تهدد كشف أو سرقة المعلومات.

و - الخصوصية (Privacy) وهي القدرة على حماية المعلومات الشخصية، والمعلومات غير المتاحة للعامة من الكشف (CSPP, 1996).

ولقد كان الكتاب ورقياً وأصبح الكترونياً ثم تحول إلى الكتاب الذي يقرأ لوحده (e-book) وما عليك إلا الاستماع إلى الكتاب وحتى الموسيقى تحولت من اشرطة إلى اقراص ممغنطة إلى ملفات (MP3). (بينيس، 2001).

رابعاً : الخصائص السياسية

يكون استخدام الحاسب في المجال الحكومي أكثر بروزاً في مجال حفظ السجلات (جمع البيانات وحفظها واسترجاعها وتحديث المعلومات)، وخاصة المتعلقة بالإنسان، والصحة، والأمن، والأحوال المدنية.

ولا تستطيع الحكومة أن تخطط خدماتها وتطورها دون معلومات، وقد وفرت الحاسبات هذه الخدمة، فالمعلومات عن السكان والصحة والدفاع والطاقة . . إلخ عنصر مهم في التخطيط الحكومي في هذه القطاعات.

استخدام الحاسب في بيان رأي المواطن في الناخب، وتحليل بيانات الناخبين ومعرفة طلباتهم واتجاهاتهم، إن بناء قاعدة من المعلومات حول سلوك الناس الانتخابي تمكن من التنبوء عن من ينتخبونه في المستقبل، ولن يحتاج المواطن في المستقبل الذهاب إلى مراكز الاقتراع والمرور بإجراءات المطابقة الأمنية والسياسية المتعبة، وإنما يمكنه الاقتراع من المنزل.

وتستخدم برامج استطلاع الرأي العام مثل برنامج CI2 و CATi وتمكن من خلال الحاسب والهاتف من سحب عينات عشوائية واستطلاع آراء الناس. ويمكن استخدام هذه البرامج في الانتخابات حيث تمكن من اعلان النتائج بسرعة كبيرة جداً.

1- اللاحدود (Noboundaries)

في مجتمع المعلومات تتلاشى الحدود السياسية والجغرافية بين الدول بسبب الربط الفضائي، ويصبح مفهوم الحدود زئبقياً، فالفرد موجود في المكان وهو في مكان آخر، هو في مكتبة الكونجرس الأمريكي يتصفح موجوداتها وهو جالس في قرية ريفية عربية. إن التطورات في عالم الاتصالات جعل مفهوم الحدود ليس ذا معنى طالما أن اجتيازه لا يتطلب إذناً أو جواز سفر أو تأشيرة دخول أو إقامة وافد. هذه الزئبقية

تزداد يوماً بعد يوم. فمفهوم المياه الإقليمية والفضاء الاقليمي جعلها كالأرض (المشاع) الكل ينافس على احتكارها واستغلالها بالاقمار الصناعية والبوارج الحربية التي تجوب هذه الأمكنة وتسترق النظر والتقدير لما هو داخل بيوتنا، جعلت مفاهيمنا الأمنية الشخصية والوطنية ليست ذات صلة. أنت تسافر وأنت موجود، وتتسوق وأنت جالس، وتخاطب الناس وترسل الفاكسات والرسائل الإلكترونية إلى كل دولة من مكان فية متسع للجميع، هذه الخاصية في مجتمع المعلومات تجعل من أمكانية وجود مجتمع عالمي واحد لا يعترف بالحدود الفيزيقية بين الدول أمراً واقعاً.

ويرى هاندي واندرسون أن المجتمعات قد انتقلت من العالم المادي (Physical World) إلى الوجود التخيلي (Virtual Existence) في الفضاء، ومن جوانب المجتمع التي انتقلت ما يلي :

أ -النشاطات المعلوماتية من مثل نشاطات التعليم، والبحث العلمي، والتصاميم الهندسية، والعمليات الصناعية، والمعلومات الشاملة، والمعلومات الترفيهية بوسائل الاتصال، والسجلات الخاصة والعامة. وغالباً ما حلت النسخة الإلكترونية محلها، وتفضل في غياب النسخ الورقية.

ب - نشاطات التحويل، يتم نقل النشاطات التجارية والتحويلات المالية، والنشاطات الحكومية من خلال الحاسب وشبكاته في غياب السجلات الورقية.

ج -الأبنية المادية والوظيفية، ويزداد ضبط هذه البنى من خلال البرمجيات والإلكترونيات أكثر من التحكم بها، وضبطها من خلال الوسائل الميكانيكية، أو الإلكترونية (Hundley & Anderson, 1994).

وهذا الحراك على مستوى المجتمع الواحد وعلى مستوى المجتمع الكوني، فالفرد يمكنه الشراء من الأمازون مثلاً بالطريقة ذاتها التي يشترى فيها كتباً من المكتبة المحلية ومن خلال الإنترنت.

2- الحكومة الإلكترونية (E-government)

لقد قامت العديد من الدول ببناء قواعد معلومات وطنية خاصة بها، وفي المجالات الحياتية المختلفة (مثل الأحوال المدنية، والإحصاءات السكانية . . . إلخ. لا بل تحولت بعض الدول إلى الحكومة الإلكترونية (مثل الامارات العربية المتحدة)، مما

يعني زيادة الاعتمادية على الشبكات في انجاز المعاملات والاتصالات . . . إلخ. إن وصول المجرمين إلى هذه القواعد وتدميرها أو تزويرها يشكل خطراً بالغاً على أمن الدولة. ولابد من الإشارة هنا إلى أهمية حماية هذه القواعد وحفظ نسخ احتياطية في أماكن متنوعة وآمنة لمواجهة مثل هذه الظروف، ومن الأمثلة على ذلك نقل ملفات الأحوال المدنية في الكويت إلى خارجها إبان حرب الخليج، ولولا وجود نسخ احتياط لعانى الكويت من مشكلة في توثيق المعلومات عن مواطنيه. وهذا يذكر بما قام به الصرب من طمس هوية الألبان في إقليم كوسوفو، وجعلوهم بلا مأوى أو هوية (Nameless & Homeless)، وذلك من خلال تدمير وحرق الوثائق الشخصية والرسمية في الإقليم والتي بحوزة السكان (CNN, 1999).

ونظراً لما جلبه المجتمع المعلوماتي من تغيرات في المجالات عامة، فقد تنبهت الدول إلى تحويل حكوماتها إلى حكومات إلكترونية لتواكب هذه التغيرات. فقد قدمت الحكومة البريطانية أكثر من مبادرة للاهتمام بتحويل المجتمع إلى مجتمع معلوماتي، وقد وضعت الاستراتيجيات اللازمة لهذا التحول. ولقد ركزت على تقديم أفضل الخدمات للمواطنين بطريقة فعالة في استخدام المصادر المعلوماتية الحكومية.

إن هذا التطبيق سيؤدي إلى بيئة لتحويل النشاطات الحكومية باستخدام التطبيقات الإلكترونية للأعمال (e-business) من خلال القطاع العام. وتقوم الحكومة الإلكترونية على أربعة مبادئ حددتها وحدة المعلومات المركزية الإنجليزية (Central Unit, 2000) بالآتي :

أ- بناء الخدمة المتمركزة حول اختيارات المواطنين (Citizen-focused government). ويتطلع المواطنون إلى خدمات بناءً على حاجاتهم، وبنوعية عالية ويسهل الوصول إليها، ومناسبة لهم وآمنة. وليس على المواطن أن يفهم كيف تعمل الحكومة، أو كيف تنظم عملها. أو ما يقوم به كل قسم في وزارة ما، وما يهم هو إيصال الخدمة إلى العميل (المواطن) بطريق مناسبة له. وهذا يتطلب المشاركة والشراكة مع القطاع الخاص في إيجاد الطرق والوسائل المناسبة.

ب- جعل الحكومة وخدماتها متاحة للمواطنين (Accessible services)، ويتطلع الناس في هذا المجال لأن تتوافر خدمات الحكومة من خلال الإنترنت، وتلفونات الجوال، التلفزيونات الرقمية، ومراكز الاتصالات، ومن خلال الحاسبات الشخصية. الخدمات الإلكترونية قد لا تكون بمعزل عن الاتصالات

الشخصية، وأن توظف حول حاجات الأفراد، وإن طريقة تنفيذ الأعمال ستؤدي إلى تغير العلاقة بين الأفراد والحكومة.

ج- شمولية الشبكات الاجتماعية (Inclusiveness) يجب أن تتطور الخدمات بحيث تكون متوافرة للجميع وسهلة الاستخدام على المستوى الفردي والجماعي، وتتوافر الخدمات على الشبكة (Online) للجميع، وهذا يشمل توفير الخدمات لجماعات الاقليات وبلغتهم.

د - إدارة المعلومات بشكل أفضل. تعد المعلومات والمعرفة الحكومية مصدراً هاماً، ولابد للقطاع الحكومي من الاستفادة المثلى من هذه المعلومات. كما ولابد من إدارة التغير في نمط الحكومة تجنباً للفوضى التي يمكن أن تحدث عن هذا التغير.

ويرى ارثر (Arthur) أنه كلما زاد الترابط بين دول العالم يضعف التحكم من المؤسسات الحاكمة، ويلاحظ خفوت الضبط الحكومي التراكمي من القرية إلى البلدة إلى الدولة (Borchgrave et. al., 2000).

خامساً : الخصائص الاقتصادية

1- الاقتصاد الإلكتروني (e-Economic)

هناك الكثير من المصطلحات الاقتصادية التي تربط الاقتصاد بالمعلومات. فالنقود قد تحولت من ورقة إلى بطاقات إلكترونية، والتحويلات المالية والعمليات المصرفية المتناقلة داخل المجتمع وبين الدول كلها إلكترونية. لقد جعلت المعلومات مكان النقود في العمليات المالية رقم حساب ورقم المبلغ والعنوان . . . إلخ. إن تعطيل، أو تخريب، أو تدمير قنوات الاتصال بين المؤسسات والأفراد من شأنه أن يهدد الأمن الاجتماعي للمجتمع بأسره.

ويعتمد الاقتصاد الحالي على المعلومات وأدواتها من حاسب إلى وسائل اتصال إلى برمجيات، ولقد بلغ رأس مال صناعات الحوسبة والاتصالات والإلكترونيات الاستهلاكية (3) تريليونات دولار، ومن المتوقع أن تضخ مليارات الدولارات في تطوير طريق المعلومات الفائق السرعة (The Information Superhighway)، ويلاحظ

أن ملامح هذا الطريق قد بدأت فعلاً في التشكل، فسباق الشركات الناقلة للاتصالات (Carriers)، تتدافع نحو المكاتب والمنازل والمؤسسات وتتنافس في تقديم أفضل الكوابل المحورية (Coax)، لتتمكن من نقل المعلومات بكافة أشكالها (صوت، صورة، تفاعل . . . إلخ). وعلى مستوى العالم فإن كلفة تشييد طريق المعلومات فائق السرعة تبلغ أكثر من تريليون دولار، من المتوقع أن تنفق اليابان (450) مليون دولار لعمل شبكة ألياف قومية بحلول العام 2015م، والولايات المتحدة (200) مليون دولار وبريطانيا (45) مليون، ولقد دخل الرئيس كلينتون البيت الأبيض من خلال طريق المعلومات الفائق السرعة حيث أعلن في حملته الانتخابية عام 1993م أنه سيجعل هذا الطريق الأساسي للبناء التحتي الأمريكي مثله مثل نظام الطرق السريعة بين الولايات الأمريكية (Interstate Highway) (كليش، 2000).

فهناك اقتصاد المعلومات (Economics of Information) فمثلاً قضى ميشلوب (Fritz Machlup, 1902-1983) حياته يقيس حجم النمو في اقتصاد المعلومات وكان عمله الموسوم إنتاج وتوزيع المعرفة في الولايات المتحدة (1962)، أساساً في قياس مجتمع المعلومات من الناحية الاقتصادية حيث ميز بين خمس مجموعات سماها :

1- التعلم (الجامعات، المدارس . . .).

2- وسائل الاتصالات (الراديو، التلفزيون . . .).

3- الآلات المعلوماتية (الحاسب . . . .)

4- تطبيقات المعلومات (القانون، التأمين، الطب).

5- الأنشطة المعلوماتية الأخرى (البحث، والتطوير . . .).

يقول دراكر (Drucker) إن المصدر الأساسي في الاقتصاد «وسائل الانتاج» بمفهوم الاقتصاد ـ لم يعد رأس المال ولا المصادر الطبيعية ولا العمال إنه وسيكون المعلومات. أن نشاطات صنع الثروة لن تكون توزيع رأس المال للاستخدام المنتج ولا العمالة . . . إن الجماعات الاجتماعية المتقدمة مجتمع المعرفة ستكون عمال المعرفة، مدراء المعرفة، والذين يعرفون كيف يوزعون رأس المال إلى الاستخدام المنتج . . . وعلى العكس من العمال في الرأسمالية فإنهم يملكون كل من وسائل الإنتاج وأدوات الإنتاج» (Drucker, 1993, p. 8).

قال نائب الرئيس الأمريكي ل جور (Gore) في شهر (ـــــ) في كلمة نادي

الصحافة الوطني :   1993
12

«اليوم تنساب التجارة ليس على الطريق السريع الإسفلتية، ولكن على الطرق السريعة المعلوماتية . . . فكر في البناء التحتي المعلوماتي الوطني كشبكة من الخطوط السريعة مثلها مثل الخطوط السريعة بين الولايات في الخمسينيات. هذه الخطوط السريعة تحمل المعلومات بدلاً من الناس والبضائع» (Gore, 1993).

بلغ حجم التجارة عبر الإنترنت (2.6) مليار عام 1997 يتوقع أن يصل إلى (37.5) مليار عام 2000م. أما التجارة العربية فقد بلغت عبر الإنترنت (9.5-11) مليون دولار(92%) منها جاءت من خارج العالم العربي (الكاملي، 1998). ويضرب رضا (1998، ص 51) المثال التالي : عندما يشتري مواطن أمريكي سيارة بونتياك لومانس من شركة جنرال موتورز، فإن هذا المشتري يقوم من حيث لا يعلم بصفقة تجارية عالمية، ذلك أن مبلغ العشرة آلاف دولار التي يدفعها لجنرال موتورز ستتوزع على النحو التالي :

- 3000 دولار إلى كوريا الجنوبية (تجميع روتيني).
- 1750 دولار إلى اليابان ثمن قطع تقانة دقيقة.
- 750 دولار إلى ألمانيا (تصميم وجماليات تصميمية).
- 440 دولار إلى تايوان، وسنغافورا واليابان ثمن قطع دقيقة.
- 250 دولار إلى بريطانيا أجور إعلان وتسويق.
- 50 دولار إلى إيرلاندا وجزيرة باربادوس ثمن معلومات.
- الباقي إلى واضعي استراتيجيات التسويق في ديترويت، وإلى المحامين، ومصرفيين في نيويورك وحاملي أسهم شركة جنرال موتورز في الولايات المتحدة وخارجها، ومن قوتها إلا أن أسواقاً أخرى أضعف منها قد شاركتها في اقتصادها.

جاء في تقرير اللجنة الإنجليزية ـ الأمريكية للتجارة الإلكترونية أن التجارة الإلكترونية ستكون محرك النمو الاقتصادي في القرن الحادي والعشرين مع إمكانية تطوير الاقتصاديات وزيادة الانتاجية وزيادة التوزيع، وتسهيل التجارة. وقد وضعت اللجنة عدداً من المبادئ المتعلقة بتسهيل التجارة الإلكترونية منها :

1- أن على القطاع الخاص قيادة التطوير في التجارة الإلكترونية وتكوين

الممارسات العملية.

2- على الحكومات التأكيد من تمتع القطاع الخاص بالبنية القانونية الواضحة والمتسقة والقابلة للتنبوء، ولكي تتمكن الحكومات من فعل ذلك فمن الضروري تجنب الغموض وعدم التيقن، أو وضع العراقيل في التجارة الإلكترونية.

3- التعاون الدولي مهم على مستوى جميع الدول في بناء البيئة المناسبة للتجارة الإلكترونية.

4- على الحكومات أن لا تضع ضرائب على النقل الإلكتروني.

5- حماية الخصوصية الفردية في التعاملات التجارية.

6- تأمين وصول جميع الناس إلى الخدمات الإلكترونية (الدول الفقيرة والغنية)

7- على الحكومات أن تشجع الوصول إلى المعلومات.

8- أن تتوافر الأدوات والنظم التي تساعد على حجب المعلومات التي لا يرغب في مشاهداتها مثل المعلومات غير المناسبة للأطفال بحيث يتمكن الفرد من اختيار ما يناسبه من المعلومات.

9- تشجيع التعاون الأمني الدولي ضد النشاطات غير القانونية على الإنترنت.

10- على الحكومات أن تقدم النصائح المتعلقة بالتهديدات أو الانكشافات في المعلومات لتأمين الاستجابة المناسبة لحماية البناء التحتي المعلوماتي.

(Conadian Interent Commerce Statistics Sheet, 2000).

2- المهن الإلكترونية (Cyberjobs)

من المقاييس الشائعة في تحديد ظهور «المجتمع المعلوماتي» هو مقياس التغير المهني، ويرتبط تحديد التغير المهني مع المقياس الاقتصادي، فمثلاً بين بوريت (Porat) أن نصف سوق العمل الأمريكي في الستينات موجود في قطاع المعلومات (Porat, 1978). يلاحظ انخفاض العاملين في القطاع الزراعي في المجتمع الأمريكي من (70%) عام 1820م إلى (50%) عام 1880م وإلى (37.5%) عام 1890، وإلى (17.4%) عام 1940، إلى (6%) عام 1960، إلى (2.8%) عام 1980م. (روسينبرج، 2000، ص 486).

ويرى ميشلوب أن هذه الفئات يمكن إرجاعها إلى إجمالي الدخل الوطني

(GNP)وبالتالي احتساب مدى مساهمة المعلومات فيه، وبناءً على ذلك فقد توصل إلى أن (29%) من إجمالي الدخل الوطني الأمريكي قد أتى من صناعة المعرفة في عام 1958م.

ويلاحظ أن المهن أصبحت (بين الحقول العلمية)، ففي الجدول التالي يلاحظ أن كل مهنة قائمة بذاتها، ويمكن تكون مهنة جديدة من أي عمودين متجاورين (مدير تخطيط)، (تخطيط النظم)، (مدير النظم)، أومن ثلاثة أعمدة (مدير تخطيط النظم) ... إلخ. ويتوقع أن تزدهر مهن في السنوات القادمة، حيث لن يكون هناك حدود للطلب على وظائف الخدمات الإنسانية، وستزدهر وظائف الترفيه (الكتاب، والممثلون، والفنانون) ذلك أن زيادة وقت الفراغ ستؤدي إلى زيادة الطلب عن أعمال الترفيه. وسيزداد الطلب على البرمجة، وعلى علماء الحاسب، وسيزداد الطلب أيضاً على السائقين، والنادلين، والخادمات، والمرافقين، والبوابين، ورجال الشرطة، والمحامين، ومعلمي الدروس الخاصة. ومع زيادة عدد المسنين سيكون هناك طلب متزايد علي موظفي الرعاية الصحية (كاكو، 2001م).

جدول رقم (6)

المهن البينية في المجتمع المعلوماتي

المهندس	الإدارة	الاتصالات
مدير	تخطيط	النظم
مصمم	العمليات	المالية
منسق	التطوير	الإبداعي
مستشار	استراتيجية	المشروع
مديـــــر	السياسة	الماليـــة
مشرف	تطبيقات	المصادر
مخطط	بحوث	الإنتاج

المصدر : البشري، والبداينة، 1999، ص 63.

ويسوق جيتس لقطة من فيلم الخريج للدلالة على موقع عصر اليوم من الماضي القريب، فيقول:

"في فيلم الخريج الذي عرض لأول مرة عام 1967 في ذلك المشهد أمسك رجل الأعمال بنيامين بيد الخريج الحديث من الجامعة... من عروة ثوبه وقدم له نصيحة طوعية في المهنة لخصها في كلمة واحدة: البلاستيك. ويتساءل جيتس لو أن ذلك

المشهد كتب الآن فهل ستكون نصيحة رجل الأعمال بنيامين كلمة واحدة: المعلومات. (ص41).

سادساً : الخصائص الأمنية

1- أمن المعلومات:

نظراً لزيادة الاعتمادية علي المعلومات في تسيير كافة النشاطات الإنسانية، فقد أصبحت المعلومات وسيلة وهدفاً وقيمة عالية في تحقيق الأهداف الاجتماعية والسياسية. ولأن الحصول على المعلومة قد أصبح أسهل وأرخص من أي وقت مضى، ولأن للمعلومة قيمة أمنية، وسياسية، وإدارية هامة، فقد أصبح الحصول عليها بالطرق المقبولة وغير المقبولة عملية هامة نجم عنها التفكير بحمايتها خاصة إذا كانت ذات قيمة أمنية، أو اقتصادية، أو تقنية عالية.

ولذا بدأ الحديث عن حماية البناء التحتي المعلوماتي وسميت بعض المكونات الهامة في هذا البناء بالبناء التحتي المعلوماتي الحساس، والذي يؤدي تعطيله أو تدميره إلى وضع المجتمع في حالة فوضى حياتية (لا ماء ولا كهرباء ولا انترنت ولا طعام ولا ثلاجات ولا اتصالات ... إلخ.). وقد استدعى هذا اهتمام الحكومات لتوفير السبل الكفيلة بحمايته، وظهرت العديد من الخطط لصيانته وبحث البدائل الدفاعية اللازمة وقت الحروب والسلام. فكما يقال لقد أصبحت الحروب الحالية حروب معلومات، ويمكن القول إن الرصاص قد استبدل بالبيانات وبالصفر والواحد، وإن الجندي قد استبدل بالدخلاء والمتسللين، والجواسيس وحتى الهواة والأطفال.

لقد بدأ الاهتمام بحماية الاقتصاد الإلكتروني والحماية ضد التجسس الإلكتروني وضد خرق الدخلاء لنظم المعلومات والحرمان من الخدمات كأمطار البريد الإلكتروني بالرسائل غير المرغوبه فيها.

لقد تبدلت المفاهيم الأمنية وحلت مفاهيم أمنية معلوماتية تتماشى مع البناء التحتي المعلوماتي، فظهر الإرهاب الإلكتروني أو الفضائي، وجرائم المعلومات، والدخلاء والمتسللون والمتطفلون ... إلخ.، وزاد استخدام العمليات النفسية والاستخبارات الفضائية، وأصبح نقل المعلومة من مكان لآخر عملية في غاية السهولة واليسر، ونقل

مليارات الدولارات عبر الفضاء دون الحاجة إلى دخول خزينة البنك، كل هذه التغيرات جعلت الأمن في المجتمع المعلوماتي مختلفاً عنه في ما قبلها. فقد تلاشت الحدود السياسية بمعناها التقليدي، وتلاشت معها تأشيرات السفر، وأصبحت الاتصالات والمواصلات تربط الكون بشكل فعال. الفضاء مشاع للجميع، وبدأت الضغوط نحو عولمة الأمن، والقانون، والسياسة، والمجتمع. وبدأت النزاعات نحو مجتمع كوني ينظر فيه إلى المجتمعات المكونة له كما ينظر إلى الأقليات داخل المجتمع الواحد، وهذا يعني تفاعل المجتمع ككل مع المحافظة على الخصوصية.

2- الجرائم الفضائية (Cybercrimes)

يعد التحول إلى الأنترنت الكونية أوما يشار إليه احياناً (I-way) من البحث الأكاديمي، والاتصالات إلى الاتصالات الكونية والبناء التحتي المعلوماتي الكوني (Global Information Infrastruction [GII]) من أهم التطورات في التاريخ الحديث، ولهذا التحول آثار في جميع جوانب الحياة الإنسانية، ومنها نظم العدالة الجنائية، ومؤسسات إنفاذ القانون ... إلخ.

ومن التغيرات الهامة لهذا العصر في مجال الجريمة والسلوكيات الإجرامية ما نتج عن تكنولوجيا (I-way)، حيث تقترف الجرائم القديمة بطرق حديثة، وجرائم حديثة بطرق قديمة، وجرائم حديثة بطرق حديثة (Boni, & Kovacich, 1999).

اتخذت الجريمة أشكالاً مستحدثة تتماشى مع البنى الاقتصادية والاجتماعية لمجتمع المعلومات، فالسرقة قد أصبحت بأشكال جديدة مختلفة عما كانت عليه في السابق، ففي المجتمع الزراعي كانت جريمة السرقة تتركز في سرقة المعدات الزراعية (أدوات الإنتاج الزراعي)، أو الإنتاج الزراعي. وفي المجتمع الصناعي أصبحت جريمة السرقة تتركز في استخدام الآلة في السرقة (سيارة، تلفون)، السطو على رأس المال بالقوة، والتي استخدمت الآلة فيها (بندقية). أما في المجتمع المعلوماتي فقد أصبحت المعلومة أداة وهدفاً في آن واحد للسرقة، فالمعلومة المتعلقة بالأداة (برنامج، برامج خرق جدران الحماية .. إلخ)، أو المتعلقة بهدف الجريمة (أرقام الحسابات)، أو كهدف للسرقة (الأسرار التجارية، والعسكرية).

لن تكون الجرائم في مجتمع المعلومات مقتصرةً على دولة بعينها، وإنما سيكون

العالم كله مسرحاً لها، حيث يمكن للفرد أن يرتكب جريمة من أي مكان في العالم وفي أي مكان. لا وجود للحدود العالمية في جرائم الحاسب خاصةً مع وجود الإنترنت، وشبكات الاتصال العالمية. وتزداد الخطورة من أن قادة الجريمة يمكنهم من توظيف طاقات إبداعية في هذه المجالات وتحت نشاطات مقبولة اجتماعيا ً ولكن بقصد توظيف واستثمار أموال الجريمة عامة، وتطوير قدراتهم التقنية الجرمية. لقد اقترح كون وفلسون أنه لتتم الجريمة لابد من حضور ثلاثة عوامل هي : (الضحية)، والمهاجم (الفاعل)، وغياب الحراسة الكلية، وبالتالي فهي لا حراسة N]o]) gurdian)، والمهاجم (A]ttaker])، والضحية (V]ictime]). (Cohen & Felsen, 1979).

ولقد استخدم ريز (Rese, 1998) ثلاثة متغيرات تصف العوامل التي ذكرها كون وفلسون وطبقها في مجال الجريمة المعلوماتية وسماتها: الأرضية (Ground)، والنتيجة (Resolve)، والمنفعة (Utility). أما الأرضية فقد تكون مادية (Physical)، أو فضائية (Cyber)، ويجب أن تكون الأرضية لصالح الحارس وتعيق المهاجم. فمثلاً شبكة الحاسب المحصنة بجدران الحماية ستعيق الهجوم وتعدي الدخلاء، وقراصنة الحاسب. أما النتيجة وهي ما يعتقد المهاجم أنه سيحصل عليه، ما يشكل جاذبية له. وأخيراً المنفعة وهي في العالم المادي «قوة»، وفي العالم الفضائي «الذكاء». وتكثر الجرائم الإلكترونية، والجريمة عن بعد، والإرهاب الفضائي، وسرقة المعدات المتصلة بالمعلومات، وتخريب البيانات والدخول غير القانوني (المشروع) للبيانات.

نظراً لتوافر تقنيات الاتصال الحديثة مثل التلفون الجوال والإنترنت، والحاسبات المتطورة والسريعة والسهلة الاستخدام، فان التحكم في إدارة العمليات (الإجرامية أو الإرهابية وغيرها) يمكن أن يكون في مكان ما بعيداً عن هدف الجريمة مثل مقتل يحيى عياش في إسرائيل بواسطة الهاتف الجوال، ومقتل زعيم الشيشان (جوهر دوداديف) بالطريقة نفسها. ومن الأخطار الأخرى في هذا المجال الوصول إلى قواعد المعلومات من خلال نشر فيروسات الحاسب فيها. إن التحكم عن بعد في الجريمة وتنفيذها أمر ممكن. وتشمل الجرائم الإلكترونية (الفضائية) على جرائم الحاسب، وتخريب المعلومات، وإساءة استعمالها أو/ وسرقتها، أو تزويرها، أو/ و انتهاك خصوصيتها والتشهير بأصحابها، والقنابل البريدية، والاحتيال المالي، وسرقة بطاقات الائتمان . . . إلخ. ويظهر ذلك جلياً من خلال وصف الـ(FBI) الجرائم الفضائية بأنها قد أصبحت وباء (epidemic) وذلك بسبب الزيادة الكبيرة في هذه الجرائم.

وتحتاج تقنيات المنظمات إلى حماية معلومات شاملة (Comprehesive

(Information Protection)، وهذا يتطلب برامج وعناصر بشرية مدربة، وسياسات، وإجراءات، وبرامج توعية أمنية.

نوع التعديات : مع تطور التقنيات فقد مكن التشفير الإرهابيين والمجرمين من أداة فعالة في تخفية نشاطاتهم، هذا بالإضافة إلى الوسائل الإلكترونية المتاحة لهم مثل الاتصالات الصوتية، والفاكس، والبريد الإلكتروني، وإمكانية تخزين البيانات ونقلها من مكان لآخر. يظهر الجدول التالي حجم الخسارة المالية الناجمة عن التعدي على المعلومات.

جدول رقم (7)

حجم الخسارة المالية للتعديات على أمن المعلومات للفترة من 1997-1999م.

مسمى التعدي	العدد	إجمالي الخسارة بالدولار
سرقة المعلومات	64	96,089,000
تخريب البيانات	66	10,848,850
التنصت	28	2,508,000
ولوج النظام من الخارج	69	7,433,700
سوء استخدام الشبكة داخلياً	203	12,302,750
الاحتيال المالي	82	75,837,000
منع الخدمة	64	6,042,000
تغيير بروتوكول الاتصال	4	512,000
فيروسات	424	25,646,150
دخول غير قانوني داخلي	40	58,123,605
احتيال اتصالات	96	40,689,300
تسجيل	6	265,000
سرقة الحاسب المحمولة	472	42,420,200
الإجمالي		360,720,555

المصدر: CSI/FBI, 1999 Computer Crime and Security Survey, p.8-9 . نتائج دراسة مسح جرائم الحاسب والأنترنت لـ (FBI/CSI) عام 1999م.

الأمن العربي في عصر المعلومات

إن المتمعن في مكونات البناء المعلوماتي في الوطن العربي والذي يشكل ركيزة مهمة في نقل المجتمعات إلى مجتمعات معلوماتية يلاحظ تأخر المجتمع العربي في هذا المجال. ففي مجال الوصول للمعلومات والاتصالات تشكل الاتصالات بنية تحتية هامة للبحث العلمي خاصة مع تزايد الاعتماد على المعلومات ونقلها وتخزينها وتبادلها. وبالنظر إلى توافر خطوط الهاتف والتلفزيون والحواسيب، والإنترنت كوحدات أساسية في البناء المعلوماتي ويلاحظ ضعف هذه البنية في الوطن العربي باستثناء الدول العربية المرتفعة في مستوى التنمية البشرية وهي (دولة الإمارات العربية المتحدة، ومملكة البحرين، ودولة الكويت، ودولة قطر) مقارنة مع العالم ومع الدول الأخرى. ويظهر الجدول رقم (8) أن معدل عدد خطوط الهاتف في العالم لعام (1990) هي 99 خطاً لكل (100) ألف شخص من السكان، يقابلها (35) للعالم العربي، و(21) للدول النامية، و(393) للدول الصناعية. وتباين هذه المعدلات في الدول العربية فأعلاها هو (247) خطاً في الكويت، و(206) خطاً في الإمارات، وأقلها (3) في موريتانيا، و(8) في جزر القمر، و(11) في اليمن، و(16) في المغرب، و(30) في مصر.

أما التلفزيون وللعام ذاته فكان معدله في العالم لكل (100) ألف من السكان (186) جهازاً، يقابلها (131) جهازاً في العالم العربي، و(95) في الدول النامية، و(502) في الدول الصناعية. أما معدل مضيفي الإنترنت فبلغ معدلها في العالم (7.42) لكل (100) ألف شخص، ومعدلها (37.86) في الدول الصناعية مقابل (0.13) في الوطن العربي.

وفي الوطن العربي هناك (16.4) أجهزة حاسب لكل (10) آلاف من السكان، ويصل هذا الرقم أعلاه في منطقة الخليج العربي (27.8) أجهزة حاسب لكل (10) آلاف من السكان، و(10.9) أجهزة حاسب لكل (10) آلاف من السكان في بلاد الشام (الاردن، وسوريا، ولبنان والعراق)، و(5.8) أجهزة حاسب لكل (10) آلاف من السكان في دول وادي النيل (مصر والسودان)، و(3.9) أجهزة حاسب لكل (10) آلاف من السكان في إقليم المغرب العربي. أما الصحف لكل (100) ألف من السكان، فوصلت إلى متوسط (77.8) صحيفة لكل (100) ألف من السكان لكل دولة في الوطن العربي، مقابل (132) في الخليج العربي، و(56) في بلاد الشام، و(32.5) في وادي النيل، و(27) في المغرب العربي.

وفي مجال الإنترنت بلغ متوسط عدد محلات الإنترنت كنسبة تقريبية من عدد السكان في الوطن العربي (28.5) لكل دولة مقابل (50.8) في دول الخليج العربي، و(26.7) في بلاد الشام، (3.6) في وادي النيل، و(٤) في دول المغرب العربي، وأخيراً بلغ متوسط عدد التلفزيونات لكل (100) ألف من السكان في الوطن العربي (207.6) لكل دولة مقابل (352) في الخليج العربي، و(152.5) في بلاد الشام، و(101) في وادي النيل، و(92) في المغرب العربي (أنظر الجدول رقم 8).

الجدول رقم (8)

مؤشر نصيب الفرد من وسائل المعلومات والاتصال

الدولة	خطوط الهاتف الرئيسية (لكل ألف شخص) 1990	خطوط الهاتف الرئيسية (لكل ألف شخص) 1998-68	خطوط الهاتف العامة (لكل ألف شخص) 1998-96	عدد المشتركين في الهاتف الخلوي(لكل ألف شخص) 1998-96	أجهزة التلفزيون (لكل آلاف شخص) 1998-96	عدد الحواسيب الشخصية (لكل ألف شخص) 1998-96	مضيفي الانترنت (لكل ألف شخص) 1998
الأردن	58	86	.06	12	52	9	0.06
الإمارات	206	389	11.1	210	294	106	7.61
البحرين	192	245	2.5	143	419	93	0.90
تونس	38	81	1.5	4	198	15	0
الجزائر	32	53	0.2	1	68	4	0
جزر القمر	8	9	0.2	0	4	-	0.01
جيبوتي	11	13	0.1	0	73	-	0.01
السعودية	77	143	2.1	31	260	50	0.02
السودان	3	6	0.1	(0)	141	2	0.00
سوريا	40	95	0.2	0	68	2	(0)
العراق	37	31	-	0	82	-	0.00
عُمان	60	92	1.6	43	595	21	0.28
قطر	190	260	1.3	114	808	121	0.02
الكويت	247	236	0.3	138	491	105	3.44
لبنان	118	194	-	157	352	39	0.74
ليبيا	48	84	0.1	3	143	-	0
مصر	30	60	0.1	1	127	9	0.04
المغرب	16	54	1.1	4	160	3	0.07
موريتانيا	3	6	0.3	0	91	6	0.01
اليمن	11	13	-	1	-	1	(0)
مجموع الوطن العربي	35	65	0.7	10	144	12	0.13
جميع البلدان النامية	21	58	1.3	18	162	-	0.26
البلدان الصناعية	393	490	4.9	223	594	255	37.86
العالم	99	142	1.9	54	253	-	7.42

(1) تشير البيانات إلى آخر سنة تتوافرعنها بيانات خلال المدة المذكورة.

المصدر : تقرير التنمية البشرية 1998، الجدول (4)، ص 201-198.

ويلاحظ من هذا الاستعراض التخلف المعلوماتي في الوطن العربي والذي يمكن وصفه بأنه مجتمع فقير معلوماتياً. فالانفاق على البحث العلمي لعام 1995م كان حوالي (872) مليون دولار من إجمالي الناتج المحلي الإجمالي (GDP) والبالغ (540) مليار دولار، أي حوالي (0.15) فقط، ومنها (89%) من القطاع العام. أما إنفاق العالم العربي على استيراد السلاح لعام 1995م، فكان حوالي (60) مليار أي ما نسبته حوالي (11%) من إجمالي الناتج المحلي (GDP). ينفق على البحث العلمي من متوسط دخل الفرد (3.2) دولار (مراياتي، 1999) (البداينة ٢٠٠١). ويظهر الجدول التالي قيمة الإنفاق على البحث والتطوير في العالم ونسبة الإنفاق في الدول المتقدمة والنامية والعربية.

جدول رقم (9)

قيمة الإنفاق على البحث العلمي والتطوير في العالم ونسبة الإنفاق في الدول المتقدمة والنامية والعربية

السنة	إجمالي الإنفاق في البحث العلمي والتطوير (مليون)	نسبة الإنفاق في الدول		
		المتقدمة	النامية	العربية
1970	6.2101	97.5	2.5	0.2
1975	113.813	95.9	4.1	0.3
1980	207.801	93.8	6.2	0.5
1985	271.850	95.2	4.8	0.5
1990	452.590	95.9	4.1	0.7

المصدر شعبان، 2000، ص (7).

أن حجم السكان العرب على الشبكة مقارنة باجمالي المستخدمين وفق اللغة منخفض جداً (0.9%) مقارنة (45%) للغة الانجليزية، (9.8%) لليابانية ويظهر ذلك جلياً من بيانات الجدول التالي.

جدول رقم (10)
حجم الاستخدام على الشبكة وفق اللغة حزيران 2001م

اللغة	النسبة
الإنجليزية	%45
اليابانية	%9.8
الصينية	%8.4
الألمانية	%6.2
الإسبانية	%5.4
الكورية	%4.7
الفرنسية	%3.4
الإيطالية	%3.6
البرتغالية	%2.5
الروسية	%1.9
العربية	%0.9

المصدر : http://glreach.com/globstats/refs.php3.

ولا يتوقف هذا الانخفاض على المشتركين، وانما يتعداه إلى محتوى الشبكة، فيلاحظ أن اللغة الانجليزية قد احتلت الغالبية العظمى لمحتوى الشبكة (68.4%)، تلتها اليابانية (9%)، والألمانية (5.9%)، ولا وجود للغة العربية حيث تشكل نسبة بسيطة جداً، والجدول التالي يبين ذلك. أما توزيع مستخدمي الانترنت ومن مناطق العالم فقد أظهر أن الولايات المتحدة تستحوذ على أكثر من نصف هذا الاستخدام (54.3%) وإذا ما أضيف إلى ذلك بقية بلدان منظمة التعاون الاقتصادي والتنمية ذات الدخل المرتفع يشكل ذلك حوالي أكثر من ثلثي الاستخدام في العالم (82.5%) . والجدول رقم (12) يبين ذلك.

الجدول رقم (11)
محتوى الشبكة وفق اللغة لعام 2001

اللغة	النسبة
الإنجليزية	%68.4
اليابانية	%5.9
الصينية	%5.8
الفرنسية	%3.9
الأسبانية	%3.0
الروسية	%2.4
الإيطالية	%1.9
البرتغالية	%1.6
الكورية	%1.4
أخرى	%2.9

المصدر : http://glreach.com/globstats/refs.php3

جدول رقم (12)
توزيع مستخدمي الانترنت وفق المناطق

الدولة	النسبة المئوية من السكان
الولايات المتحدة	54.3
بلدان منظمة التعاون الاقتصادي والتنمية ذات الدخل المرتفع (باستثناء الولايات المتحدة)	28.2
أمريكا اللاتينية ومنطقة البحر الكاريبي	3.2
شرقي آسيا ومنطقة المحيط الهادي	2.3
أوروبا الشرقية ورابطة الدول المستقلة	3.9
الدول العربية	3.9
أفريقيا جنوب الصحراء الكبرى	0.4
جنوب آسيا	0.4

المصدر: مكتب تقارير التنمية البشرية / برنامج الامم المتحدة الانمائي

الجزء الثاني:

حرب المعلومات: التطور والنظرية

- الفصل الرابع : تطور حرب المعلومات.
- الفصل الخامس : حرب المعلومات: النظرية
- الفصل السادس : حرب الخليج وأسلحة التخريب الشامل

تمهيد

يتناول هذا الجزء تطور حرب المعلومات وماهيتها ونظريتها. شمل هذا الجزء ثلاثة فصول هي: الفصل الرابع حرب المعلومات: التطور والنظرية. وقد عالج هذا الفصل التطور التاريخي والاجتماعي لحرب المعلومات. وحرب المعلومات في الاسلام والتطورات المقبلة للمعلومات عامة ونشاطات حرب المعلومات، أما الفصل الخامس تناول نظرية حرب المعلومات، حيث بدأ هذا الفصل باستعراض مفهوم حرب المعلومات، كما شمل هذا الفصل انموذج توفلز في وصف تارخ الحروب. وأخيراً تناول هذا الفصل بشيء من التفصيل نظرية دورثي داينّنج في حرب المعلومات. أما الفصل السادس تناول بالتفصيل حرب الخليج الثانية كأول حرب معلومات والأساليب التي استخدمتها أطراف الصراع فيها.

الفصل الرابع

تطور حرب المعلومات

مقدمة

يتسم عصر المعلومات بالاعتمادية المتزايدة للمجتمعات اليوم على المعلومات وفي كافة الأنشطة الحياتية المختلفة الرسمية منها وغير الرسمية، المدنية والحكومية والعسكرية. وتقدر قيمة المعلومات التي يتم تبادلها يومياً بمليارات الدولارات. ومع بداية التسعينيات بدأ الغرب الاهتمام بأمن المعلومات وحرب المعلومات حتى أن راثمل (Rathmell) سمّى المعلومات أسلحة التخريب الشاملة (Weapons of Mass Corruption).

الثورة المعلوماتية هي ثورة اجتماعية أصابت تغيراتها كافة النظم الاجتماعية، وحولتها إلى أبنية جديدة في السياسة وفي التجارة وفي الضبط الاجتماعي، وبالتالي لم تقتصر آثار ثورة المعلومات على نظم الاتصالات والمواصلات بل تعدتها إلى نظم العلاقات الإنسانية وحولتها من تفاعلات واقعية وفعلية إلى تفاعلات تخيلية يصعب فيها أحياناً فصل الواقع عن الخيال أو الخيالات.

ويمكن مقارنة السرعة الفائقة لانتشار المعلومات من خلال المقارنة التالية، لقد استغرق الاستخدام الأمثل للراديو (35) سنة، وللتلفزيون (13) سنة، وللانترنت (4) سنوات. وقبل أقل من (10) سنوات كانت رقائق الحاسب تحتوي على (1.1) مليون ترانستور، أما اليوم فهي تحتوي (120) مليون، وهناك محاولات لرفع هذا الرقم إلى (1) مليار (Ehlers, 1999).

المعلومات قوة وهي ذات قيمة غالية وعالية في وقت السلام والحروب. ففي السلام يتركز التنافس على المعلومات في الحصول عليها بطرق مقبولة اجتماعياً وغير مقبولة اجتماعياً (التجسس الاقتصادي والصناعي والتجاري)وفي وقت الحروب يتركز الحصول على المعلومات بطرق منوعة منها من خلال التجسس بكافة أشكاله والذي لايتوقف على أوقات الحرب ولكنه يستمر خلال السلم. هذه الأهمية لا تتوقف عند تقدير ما لدى الطرف الآخرمن إمكانيات ولكن كيف تحول الطرف الآخر من ند إلى ضحية من طرف يُقاتِل إلى طرف يُقاتَل وهو مسلوب الإمكانيات الرئيسة في القتال، وكيف تسبب انهيار جَبهته الداخلية التي تشكل السند الرئيسي له في الحرب. لم تعد الحروب بين الجيوش فقط، لقد أصبحت الحروب عن بعد، وأصبحت الحرب شاملة، لم تعد تحكمها أخلاقيات حرب أو معاهدات جنيف فتدمير البنى التحتية المدنية، وضرب المدن، وشن العمليات النفسية على المدنيين، وتدمير مؤسسات الإعلام، والمستشفيات، والقرصنة البحرية... . . . إلخ. أصبح هذا كله سمة من سمات الحروب الحديثة على أساس أن ذلك يصب في دعم المجهود الحربي، وتدميره يضعف المعنويات ويحطم الإمكانيات للطرف الآخر.

تطور حرب المعلومات

بدأت مقدمة صفحة ال (FAS) الالكترونية بـ

".....لم يعد العالم يسير بالحروب، أو بالطاقة، أو بالمال، إنه يُسيَّر بالآحاد والأصفار الصغيرة، بالقليل من البايتات الصغيرة، إنها جميعها إلكترونيات . . . هناك حرب في الخارج . . . وهي لا تتعلق بمن يملك العتاد الأكثر . . . إنها تتعلق بمن يسيطر على المعلومات. ان ما نراه ونسمعه، وكيف نفكر، كل ذلك يتعلق بالمعلومات (FAS, Homepage).

كانت المعلومات تشكل دائماً عنصراً هاماً في الحرب، ولكنها لم تكن في السابق تشكل العنصر الأهم في الأولويات العسكرية ، ففي المجتمع الزراعي كانت الأولويات في المحافظة على مصادر الزراعة وأدواتها من الماء والأرض والمحصول. . . إلخ. وفي المجتمع الصناعي كانت الأولية المحافظة على المصنع والعمال والآلة . . . وفي مجتمعات الموجة الثالثة تحتل المعلومات أعلى قيمة استراتيجية لها عبر تطورها. وهذا يعني أن المعلومات تشكل تهديداً أمنياً بالغ الخطورة للمجتمع المعلوماتي في هذا العصر، فهي أداة ووسيلة ومصدر هام في حرب المعلومات.

إن حرب المعلومات ليست جديدة. وهي ليست ظاهرة "الموجة الثالثة"، أو من نتاج ثورة الكمبيوتر. بل إنها ليست جديدة على الجنس البشري. والأمثلة من الطبيعة كثيرة فبعض الطيور مثلاً، و الذي يستخدم منها المعلومات قد ضلل أكثر من (180) نوعاً من الطيور بوضع بيضه في أعشاش الطيور الأخرى ويُكرهها على حضانتها، ولمحاولة منع اكتشافه، يحاول هذا الطائر تعديل شكل البيضة لتصبح مثل بيضة الطائر المُضيف، وبسلوكه هذا يدمر تكاملية بيئة معلومات المُضيف. ويصبح المظهر الخارجي للبيضة مصدر معلومات غير موثوق به ومُضلل. وهناك مثال آخر فإن "الغراب" يقوم بحركات استسلام خادعة كاذبة للمناوئين الذين يكرههم كي يشجعهم على الاقتراب منه، فإذا اقتربوا منه قام بهجمة شرسة عليهم. وتقوم النباتات والحيوانات الأخرى أيضاً باستخدام طرق مشابهة للدفاع عن نفسها باستخدام حرب المعلومات الدفاعية لحراسة المعلومات الهامة لحياتها (Rue. 1994). فالأسماك والأفاعي تغير شكلها وتأخذ شكل البيئة التي تعيش فيها لحمايتها من الأعداء. وهناك نباتات تعيش على نباتات أخرى (الطفيليات)، تسرق غذائها من النبتات الأخرى بدون موافقتها وتاخذ شكلها، ونبتات أخرى تستخدم الخداع في اصطياد الحشرات، فإذا ما وقفت الحشرة على النبته أنقضت عليها وأطبقت أغصانها وقتلتها وامتصت محتوياتها. ولقد استخدم

الانسان على مر العصور أساليب التمويه والاخفاء، والخداع.....الخ في صراعه مع الانسان والطبيعة.

وهكذا، فمع أن حرب المعلومات أمر ليس جديداً، إلا أنها تحولت الآن إلى أشكال وتقنيات جديدة. ولم يكن يفكِّر المحارب في بداية القرن العشرين أن يصبح التسلل من خلال أجهزة الكمبيوتر وشبكاته ونظمه لسرقة الأسرار، وإطلاق فيروسات الكمبيوتر الوبائية القاتلة على شبكات الكمبيوتر لتعطيلها، أو يستقبل مكالمات الهاتف الجوال، أو الحصول على معلومات بالتجسس من خلال صور الأقمار الصناعية أو من خلال الدعاية باستخدام محطات الإذاعة والتلفزيون. فلم تكن هذه التقنية قد تم التفكير فيها أو إيجادها بعد في مطلع القرن العشرين. ومع حلول الخمسينات من هذا القرن تمَّ اختراع الكمبيوتر والراديو والتلفزيون، إلا أنها لم تنتشر كثيراً بين الناس، ولم يكن أحد قادراً على الاتصال بها من بُعْد. ولم تكن هناك مواقع على الشبكة العالمية يمكن التسلل إليها، ولم يكن هناك مقدمو خدمات الإنترنت على الشبكة، ولم يكن هناك عمليات يمكن التصدي لها على الإنترنت، ولم يكن هناك البريد الإلكتروني الذي يمكن اعتراضه وفتحه لقراءته والتعرف على أسراره ومحتوياته، أو استخدامه لبث فيروسات تخريبية قاتلة. ولم تكن هنالك طرق رخيصة التكاليف تُمكن الفرد من إيصال رسالته إلى ملايين البشر بسرعة هائلة، وقد تحتوي الرسائل على فيروس مؤذٍ، كما أشرنا، أو رسالة ناقمة أو كذبة صارخة أو نظريات تآمر.

إن تاريخ حرب المعلومات قد وصف في ثلاث موجات، فخلال الثورة الزراعية كانت الحرب تعتمد على أدوات مبنية على الزراعة، وفي الثورة الصناعية تغيرت الحرب إلى الدمار الشامل، أما في عصر المعلومات فقد تحولت الحرب إلى حرب المعلومات، فلم تعد القدرة التدميرية الشاملة هي الأساس بل القدرة التدميرية للبيانات والمعلومات وأدواتها، هجمات معلوماتية بأقل عدد من الخسائر البشرية، وفي ساحة المعارك فلا زالت تقنيات المعلومات تستخدم لجعل الأسلحة أكثر (ذكاءً) لتقليل الخسائر البشرية، وأصبح الاعتماد على المعارك (جو - أرض) والاعتماد على بنية السيطرة المتمثلة في الاتصال والسيطرة والتحكم والمعلومات (C3I)، أو بإضافة الحاسب (C4I). ومن أسلحة حرب المعلومات المحتملة فيروسات الحاسب (الديدان، وحصن طروادة، والقنابل المنطقية، ومصائد الباب الخلفي، وآلات النانو والميكروبات، والتشويش الإلكتروني وبنادق HERF، وقنابل EMP).

وفي السابق كان على الفرد أن يتجسس وينصت ويسجل المكالمات لكي يحصل على معلومات شخصية، أما الآن فقد أصبحت غالبية المعلومات متاحة من خلال المصادر المفتوحة، أو من خلال قواعد المعلومات. إن غالبية الناس لا يفضلون وينزعجون من نشر معلوماتهم للعامة، خاصة المعلومات التي تتعلق بالصحة والمرض

والدخل وأرقام الحسابات والأرصدة، والقروض، والأدوية، والسجلات الجنائية، والاعتقال، وسجلات المحكمة، ولا يفضل الناس وصول مثل هذه المعلومات حتى للأصدقاء، والمشكلة أنك قد تقضي حياتك تدافع عن نفسك بعدم صدق المعلومات في الوقت الذي لا يُعرف من وضعها على الشبكة أومسؤول عن وضعها هناك.

وقد كان الإنسان ولا يزال مهتماً بحماية معلوماته ضد أعدائه. فقبل أكثر من (5000) خمسة آلاف سنة، حمى إمبراطور الصين سر إنتاج الحرير، أو دودة القز التي تنتج ألياف الحرير الطبيعي، وشجر التوت الذي يُعد الغذاء الأساسي والمسكن المناسب لدودة القز، وأسلوب نسج هذه الألياف لصناعة خيوط الحرير الطبيعي، وقد هدد الإمبراطور من يبوح بسر صناعة الحرير بالقتل تعذيباً. وقد نفعهم هذا النظام الأمني الشديد لمدة وصلت حوالي ثلاثة آلاف سنة، حيث نقل هذا السر أميرة غادرت الصين لتتزوج أميراً في دولة بعيدة. ففي عام (1500) قبل الميلاد أيضاً احتفظت حضارة ما بين النهرين بأسرار صناعة الفخار الملون ولكن بطريقة أقل تهديداً لحياة البشر. وقد كتب الصناع طريقة صناعتهم للفخار الملون على شكل رموز واحتفظوا بها في قطعة من طين الفخار. وفي القرن الأول قبل الميلاد، خاف يوليوس قيصر أن تكتشف رسائله فكتب إلى سيسار (Caesar) وأصدقاء آخرين رسالة سرية مرمزة لا تزل تحمل اسمه حتى اليوم (Denning, 2000 b).

ويمكن العثور على أمثلة عن حرب المعلومات خلال التاريخ البشري. فحوالي سنة 1200 قبل الميلاد، دخل اليونانيون متسللين إلى طروادة بطريقة مخادعة حيث استخدموا حصان طروادة الشهير. ومن كان يظن أن ذاك الحصان الخشبي كان طريقة تمويه ويحوي في داخله على عدد من المقاتلين المسلحين؟ وفي القرنين الثاني عشر والثالث عشر الميلاديين نجح المغول في إلحاق الهزيمة بكل من الإمبراطورية الصينية، والمسلمين والنصارى حيث درسوا المواقع الدقيقة لأعدائهم بينما استطاعوا في المقابل الاحتفاظ بأسرارهم القتالية. وفي معركة لينتز حيث تحالفت القوى البولونية والبروسية ضدهم، استطاعوا الانتصار على جيش قوامه أربعة أضعاف عددهم. فقد استطاعوا المحافظة على معرفتهم المتينة بنظام القوى المتحالفة ضدهم، بينما أغروا أعداءهم أن يلحقوا بسرايا صغيرة من جيشهم مما جلبهم إلى الجيش الأساسي للمغول، فقضوا عليهم. وكذلك خلال حروب نابليون قطعت البحرية الملكية البريطانية اتصالات البحر الاستراتيجية لبعثة نابليون إلى شمال أفريقية مما أدى إلى هزيمته (Denning, 2000b). وتاريخياً فقد استخدم هانيبال (Hannibal) إشارات المرآة خلال الحرب الثانية (Punic War) لمتابعة تحركات الرومان، وكان يفاجئهم ويخدعهم في كل مرة (Arquilla, 1994). ولقد أصبحت السيطرة المعلوماتية أو التفوق المعلوماتي (Information Dominance) عنصراً أساسياً في كسب الحرب .

ولقد استخدم المسلمون أساليب متعددة يمكن أن تقع ضمن أساليب حرب المعلومات الحديثة وخاصة ما يتعلق بالعمليات النفسية. فقد استخدم المسلمون أساليب تحطيم الروح المعنوية لدى الأعداء ، قال (ﷺ) «جاهدوا المشركين بأموالكم وأنفسكم وألسنتكم»، وقال (ﷺ) «إن المؤمن يجاهد بسيفه ولسانه، والذي نفسي بيده لكأن ما ترمونهم به نضح النبل». وإيقاع الرعب والخوف من الأساليب النفسية الأخرى التي استخدمت، قال (ﷺ) «نصرت بالرعب»،

ولقد استخدمت أساليب أخرى منها الصدق في القول والتصميم على تحقيق الهدف، وحيث كان القادة المسلمون يحذرون العدو وينفذون وعيدهم، وذلك لإحباط إرادة القتال، ولقد استخدم الأمريكان هذا الأسلوب مع العراق من خلال النشرات الورقية التي تحدد تاريخ ووقت تدمير مواقع عسكرية معينة وكان يطلب من الجيش العراقي الهروب منها. كما أن المسلمين قد استخدموا الجواسيس في جمع المعلومات، فقد وجه مروان بن محمد ابنه عبد الله لحرب الضحاك بن قيس الشيباني وأرسل له رسالة جاء فيها «احذر أن يُعرف الجواسيس في عسكرك أو يشار إليهم بالأصابع . . . وأعلم أن لعدوك عيوناً راصدة وجواسيس كامنة وأنه من يقع رأيه عن مكيدتك بمثل ما تكايده به»، كما استخدمت الخدع ويقول الرسول (ﷺ) «الحرب خدعة . . .» وقيل «رب حيلة انفع من قبيلة» .

ولقد استخدمت أساليب الحرب النفسية على نطاق واسع لتشكيك العدو بالهدف الذي يقاتل من أجله، فمثلاً في فتح مكة تم التركيز على المباغتة وإخفاء أمر الهجوم وتدمير معنويات العدو، وبث الفرقة بين صفوف العدو، وتحييد القوى الأخرى وحرمان العدو من محالفتها والتخويف والضغط النفسي من خلال استخدام كلمات وصيحات مثل « الله أكبر» و«أحد أحد»، والطلب من أفراد العدو إلى التسليم في مقابل المحافظة على حياتهم، ففي فتح مكة أعطى الرسول الأمان لقريش على لسان أبي سفيان «من دخل دار أبي سفيان فهو آمن، ومن أغلق بابه فهو آمن، ومن دخل المسجد فهو آمن»، ولقد استخدمت بعض هذه الأساليب في حرب الخليج الثانية حيث طُلب من الجيش العراقي التوجه إلى إخوانهم في السعودية وأنهم ان حملوا ورقة «العبور الآمن» فلن يؤذوا ولهم الحياة والمعاملة الحسنة . . . إلخ.

كما أن المسلمين قد استخدموا العيون والأرصاد لجمع المعلومات عن الخصم وتحركاته، وكان للنبي (ﷺ) عيون في المدينة مثل حذيفة بن اليمان، وفي مكة

العباس، وفي القبائل العربية. كما تم استنطاق الأسرى واستجوابهم وجمع المعلومات منهم، ففي معركة بدر قبضت جماعة استطلاع على غلامين يستقيان عند ماء بدر فتولى النبي استجوابهما وسألهما : كم ينحرون من الجزر (الإبل) كل يوم؟ فقالا يوماً تسعة ويوماً عشرة، فاستنبط الرسول من ذلك أنهم بين (900-1000 شخص) لأن من عادات العرب أن تخصص بعيراً لكل (100 شخص)، وكذلك تعلم لغة العدو، قال (ﷺ) «من تعلم لغة قوم أمن شرهم»، كما استخدمت الرموز والثغرات، ففي غزوة الخندق بعث النبي (ﷺ) بعض رجاله إلى بني قريظة ليعرفوا حقيقة ما بلغه من نقضهم العهد وهم داخل المدينة وأمر بأن يلحنوا بالقول وحين يعودون ولا يفصحوا في حالة تأكدهم من الخبر.

وفي عام 1912 عندما قطع الإنجليز كوابل الاتصال الخمسة الألمانية التي ترتبط ألمانيا مع العالم الخارجي (اثنان مع Azores وأمريكا الشمالية وواحد مع Vigo وواحد مع Tenerife وواحد مع Brest)، شكلت هذه الخطوة حرب معلومات، حيث يعلم الإنجليز أهمية المعلومات والاتصالات، وكان الهدف هو إضعاف قوة الألمان في الاتصال والتحكم والسيطرة (Headrick, 1991). وكذلك الحال عندما اعترضت الولايات المتحدة شفرة اتصالات المخابرات اليابانية المتعلقة بالعمليات الحربية والمفوضيات الدبلوماسية فقد شكلت هذه حرب معلومات (Branford, 1982).

يقول سولفان ودوبك (Sullivan & Dubik):

«لكي تنجح "تنتصر" على دولة صناعية فإن ذلك يتطلب عامة ليس تدمير الجيش لوحده ولكن تدمير البنية العسكرية، وقواعد المصادر والتصنيع والمساهمة في المجهود الحربي الكلي. ان تحقيق نصر ضد دولة معلوماتية يتطلب تدمير قواعدها العسكرية وما يصنع قدرتها الحربية (وهذا ربما يشمل أهدافاً صناعية ومعلوماتية) ونظمها المعلوماتية» (موثق في Devost, 1995, p. 10).

وفي مجتمع المعلومات، فإن نظام تحديد الموقع الجغرافي (GPS) يوجه الصواريخ إلى مسافات بعيدة جداً ودقيقة في إصابتها. وهذا يعني إمكانية تدمير مستودعات الذخيرة، وصواريخ العدو، وطائراته. إن المنتصر في الحرب العالمية الثالثة والرابعة هو من يقف على قدميه أولاً، وبالتالي فإن وزارة الدفاع الأمريكية ترى أن يزود العلماء

بطريقة لإعادة بناء المجتمع بسرعة، وعدم إعاقتهم بتعقيدات غير ضرورية، وهذا يعني وجود شبكة من دون شرطي(الإنترنت) فالقواعد البيروقراطية، والرقابة، والتدخل الحكومي يمكن أن تؤخر بناء أمريكا في سباقها مع الروس، وهذا أحد الأسباب لبناء الإنترنت دون رقابة وقواعد، وتعليمات (كاكو، 2001م).

وفي تقرير قدم إلى مكتب المحاسبة العامة (GAO) عام 1996م، إفاد أن وزارة الدفاع يمكن أن تكون قد تعرضت إلى (250) ألف اختراق هجوم في عام 1995م، وكانت محاولات الهجوم ناجحة في (65٪) منها وأن عدد حالات الهجوم في زيادة، وتزداد تعقيداً نظراً لاتساع مكونات البنية التحتية المعلوماتية ولزيادة مهارة الدخلاء وقراصنة الحاسب ومجرميه (GAO/AIMD, 1996).

وقد يأتي اليوم الذي يصبح فيه كل جهاز، بل وكل عملية، مرتبطاً بالشبكة العالمية. وإن مضامين حرب المعلومات دقيقة جداً. فهل سيستطيع المتسلل إلكترونياً، والذي ربما يكون في الطرف الآخر من الكرة الأرضية، قادراً على تعطيل نظام أمن المطار، أو فتح البوابات في مجمع عسكري؟ هل يستطيعون إيقاف محرك سيارة تسير بسرعة (210 كلم) على الطريق السريع، وبالتالي تسبب اصطدام مئة سيارة تمشي خلفها، أو تغيير طريق السير على الطريق السريع؟ وهل سيستطيع اللصوص والمستأجرون للقتل تتبع حركة ضحيتهم من خلال صفحات مواقع الإنترنت بحيث توفر لهم صور الأماكن العامة أو تفاصيل البيوت من الداخل؟ (Denning, 2000b).

ستصبح تقنيات المعلومات محمولة في جيوبنا وعلى أجسامنا على شكل "بطاقات ذكية" تحمل ضمنها معلومات شخصية عن كل شخص يحملها، وأجهزة الاتصالات المحمولة كالهاتف الجوال، والنداء، وخدمات البريد الإلكتروني، ومعدات الحقيقة التخيلية وأجهزة تحسين السمع وغير ذلك من الأجهزة الجسمية. ويقوم عمال في شركة بوينغ للطائرات في أيفريت بواشنطن باستخدام تجهيزات جاهزة التصنيع للحقيقة التجميعية. وتشتمل كل بزة من هذه الملابس نطاقاً للخصر يشتمل على جهاز حاسب شخصي يعمل بموجب برنامج وندوز، وغطاء للرأس يشتمل على جهاز لتحديد الموقع وشاشة للعرض. ويشتمل إعداد الجهاز على يد توجيه إلكترونية تخلص العامل من النظر إلى المخططات الورقية وقوائم قطع الغيار. وعندما يصل هذا الكتاب إلى المطبعة ستقوم شركة متعاونة مع شركة سوني للإكترونيات ببيع جهاز كمبيوتر

عالي الطاقة يمكن ارتداؤه يسمى: "المساعد المتحرك". ويمكن تشغيل هذا الجهاز الذي يبلغ وزنه كيلوجرام واحد بالصوت، ويستخدم مع شاشة تحمل على الرأس. وبإمكان مستخدمي هذا الجهاز إجراء مكالمات هاتفية، وإرسال فاكسات والاتصال مع شبكة الإنترنت. فإذا استطاع عدو اختراق هذه الأنظمة، ولنفترض أنه طلب تغيير محتويات شاشة العرض، فما هو التأثير الذي سيحدثه هذا الاختراق على حامل هذا الجهاز؟ (Nash, 1997).

وقد يأتي اليوم الذي نرى فيه شرائح الكمبيوتر تتخاطب مباشرة مع خلايا الدماغ البشري. وقدتربط مثل هذه الشرائح بآلات تصوير صغيرة جداً مع الدماغ لتساعد المكفوفين على الإبصار والرؤية، أو يمكن استخدامها لتعزيز ذاكرتنا البشرية وعملياتنا الدماغية. ويقوم الآن الباحثون في معهد التقنية في كاليفورنيا بإجراء تجارب على شرائح سيلكونية (رملية) تمَّ ابتكارها باستخدام تقنيات الدوائر المتكاملة المعروفة. ولقد تمَّ زرع الشرائح ضمن (16) فجوة تبلغ سماكة كل منها نصف قطر الشعرة البشرية، وملئت بمواد مغذية للأعصاب وخلايا عصبية مستقلة من أدمغة جرذان. وقد نمت استطالات للنيورونات على جدران الخلايا واتصلت ببعضها، كما هي الحال في الدماغ المتطور. وأما المناطق الموجودة بين الخلايا العصبية، والتي تشبه الممرات الكهربائية التي تحاكي الذاكرة الموجودة في الدماغ فيتم اكتشافها بواسطة الكهروب المرتبط بالفجوات. ويتم ربط الكهروبات بكمبيوتر يحلل عوامل الاتصالات العصبية. ويقول الباحثون: يمكن أن تُسْتَخْدَم هذه الشرائح في نهاية المطاف لتعزيز مختلف العمليات الدماغية (Weiss, 1997).

تصور شريحة دماغية ترتبط مع شبكة الإنترنت باتصال لا سلكي تتيح لنا رؤية الناس والأمكنة على الطرف الآخر من الأرض والمحادثة باستخدام الصوت والبريد الإلكتروني ويمكن الاتصال مباشرة بالمعلومات الموجودة على صفحات الإنترنت. وستكون حرب المعلومات ذات صورة جديدة مختلفة تماماً عمَّا هي عليه الآن، وليست بالصورة التي يمكننا الآن التعامل معها. فقد يكون من الممكن تصور الفيروس الذي يتسبب بإصابة الحاسب الشخصي وإلحاق أضرار بمحتوياته، إلا أننا لا يمكننا أن نتصور إلحاق الأذى عن طريق فيروس يزود الدماغ البشري بالمعلومات التي يريدها. وقد تفتح الشرائح الدماغية أشكالاً جديدة من العمليات النفسية (Denning, 2000b).

يتمنى نيل جرشنميلد مدير مشروع «الأشياء التي تفكر» الذي يرى الأشياء غير الحية تفكر، وقد اكتشف طريقة للإحساس بالوجود، فالفضاء حول أجسامنا مشحون بحقل كهربائي غير مرئي مثل شبكة العنكبوت، وعندما تتحرك أجسامنا يتحرك هذا الحقل كالهالة ، ويمكن استثمار هذه الهالة بوجود أجهزة استشعار، ويري أن أحد المجالات المهملة هي الأحذية التي نلبسها، ويمكن لها أن تقوم في المستقبل مقام بطاريات الحاسب، فوجود (80) واط في حجم الإنسان يمكن الاستفادة منه، ويمكن وضع شفيرة في الحذاء لنقل المعلومات الشخصية للآخرين، فيمكن نقل السيرة الذاتية من الحذاء إلى الأيدي، ويمكن أن يكون شعار الأشياء التي تفكرهو : «لقد أمكن للأحذية في الماضي أن تتعفن، ويمكن لها في الحاضر أن تلمع، أما في المستقبل فيمكنها أن تفكر بكمبيوتر في الملابس» (كاكو، 2001، ص 50).

ولقد أنشأت التقنية الحديثة للمعلومات العديد من الاحتمالات للهجمات المستخدمة في حرب المعلومات. ويمكن أن تحدث العمليات في أي لحظة، كما يمكن أن تنطلق من أي مكان في العالم. فيمكن إعداد هذه الهجمات وتنفيذها من مكان الاستمتاع والراحة في البيت، أو المكتب، ودون الحاجة إلى تكاليف الجواسيس، والاختراقات الفعلية والتعامل مع المتفجرات. كما أن عدد الأهداف التي يمكن الوصول إليها هو عدد مذهل. ويمكن أن يقوم بهذه العمليات ممثلون حكوميون أو غير حكوميين، ومن قبل الأفراد أو الجماعات. كما أن تكلفة هذه العمليات قد تكون تافهة تماماً، وأما الخسائر التي تلحق بالضحايا فهي موجعة. إن تمويل العمليات العسكرية العادية هو أمر مكلف. وقد تبلغ كلفة طيارة نفاثة مقاتلة واحدة أكثر من مئة مليون دولار. ومن ناحية أخرى، فهناك تكلفة أخرى لكل من شرائح الكمبيوتر، وخزانات الوقود، والأقمار الصناعية للتجسس والقوات المسلحة الهائلة. وبالمقارنة، فإن مبلغاً يتفاوت ما بين (1-10) ملايين دولار يمكن أن يكون مبلغاً مربحاً جداً لتمويل فريق حرب معلومات تقني برواتب مغرية، بحيث يتألف الفريق من (10-20) من المتخصصين بعمليات التسلل عبر أجهزة الكمبيوتر وشبكاته باستخدام آخر ما توصلت إليه تقنية الحاسبات الآلية. كما يمكن تحميل الأدوات التي يستخدمها هذا الفريق الفني في أعمالهم التسللية إلى أجهزة الكمبيوتر وشبكاته مجاناً من مواقع مختلفة على الإنترنت في مختلف أرجاء العالم. ولكن، هل يستطيع هذا الفريق

التقني المتخصص تحقيق الأهداف ذاتها التي تحققها القوات العسكرية المعروفة وتسبب استسلام العدو أو قبوله للأمور السياسية المفروضة؟ وهل يجد الأعداء أن إرهاب المجتمع بهذا الشكل هو مناسب لما يدفعونه من تكاليف عالية؟ (Denning, 1999).

ويلاحظ أنه تتزايد أتمتة الهجمات التي تهدف إلى حرب المعلومات. كما أن هناك برامج موجودة على الإنترنت تساعد في كشف كلمات السر أو العبور إلى الشبكات المختلفة والتنصت على الاتصالات وإغلاق أجهزة ملقمات أو خادمات شبكة الإنترنت، ومسح كافة الأدلة الموجودة على الأعمال غير القانوينة. كما أن هناك بعض البرامج السهلة الاستخدام لتحقيق هذه الغايات والتي تتعامل من خلال واجهة بينية رسومية. ولا شك أنه لا بد من امتلاك المعرفة الأساسية بتشغيل البرامج وإطلاق الهجمات المطلوبة، وأن يكون العامل في هذا المجال إما "عبقرياً" موهوباً في مجال الكمبيوتر، أو حاصلاً على درجة في الحاسبات الآلية وعلومها.

ويتوقع دان باركر، وهو شخص متقاعد ومحارب قديم من المتخصصين في عالم الجريمة في الكمبيوتر، يتوقع أن يأتي اليوم الذي تصبح فيه الجريمة "مؤتمتة"، حيث يستطيع الفرد تحميل البرنامج الذي يريده من الإنترنت أو يشتريه من موقع من مواقعها ويقوم البرنامج بمختلف الخطوات التي تنفذ الجريمة دون ذكر اسم المجرم أو عنوانه أو أية تفاصيل عنه، ثم يقوم البرنامج ذاته بعد ذلك بمسح كافة آثار الجريمة بحيث لا يبقى لها أثراً على الأجهزة التي دخل إليها للضحية. وإن مثل هذه البرامج التي يمكن تسميتها: "التزوير-في-العلبة" يمكن أن تحمل عناوين مثل: "تزوير شيكات قوائم الرواتب"، أو "البريد السريع للتخريب". كما أن امتلاك برنامج من هذا النوع لتنفيذ الجرائم هو أمر قانوني، وأما استخدامه وتنفيذه فلن يكون قانونياً، إلا أن احتمال إلقاء القبض على أمثال هؤلاء المجرمين بالجرم المشهود ومتلبسين بالجريمة يكون ضئيل الاحتمال جداً. وستكون هذه البرامج مؤتمتة وآلية في كل خطوة من خطوات العمل والتنفيذ بدءاً من اختيار الضحية إلى تنفيذ الجريمة وإزالة آثار العدوان والجريمة. ويمكن أن يتم تصميم أمثال هذه البرامج بحيث لا يعرف المجرم ضحيته، ولا يعرف نوع الجريمة التي سيتم ارتكابها بالتحديد، ولا الطريقة التي ستستخدم لارتكاب هذه الجريمة، وكل ما يعرفه أنه سيحصل على مبلغ مليون دولار مثلاً، يوضع في حسابه البنكي خارج حدود البلد التي ينتمي إليها. كما يحتمل أن يشفِّر مطور البرنامج

برنامجه بحيث يتجاوز كافة قوانين العقوبات على الجرائم، وقواعد تحري آثار الجريمة واكتشافها، والإجراءات القانونية التابعة لذلك (Parker, 1997).

وأما ديفيد بوني (Boney) فقد طور تصميماً رفيع المستوى لأداة برمجية يمكن استخدامها لاختبار إمكانية تعرض البنية التحتية في بلد ما لأخطار المهاجمة باستخدام برامج الكمبيوتر والشبكات المتصلة به باستخدام هجمات حرب المعلومات، أو لشن هجمة فعلية. ويقوم جيش من عملاء برمجة بعملية هجوم على برامج البنية التحتية للبلد بتوجيه من أمر تمَّ توزيعه. وإن أداة برمجية من هذا النوع هي في منتهى الفائدة والنفع، بل قد تكون أساسية لبرنامج دفاعي كبير، إلا أنها أيضاً قد تسهِّلُ هجمات فنية على مستوى رفيع ومعقد من قبل أعداء عاديي المستوى والقدرات الفنية (Boney, 1997).

ونحن نلاحظ أن التقنيات الحديثة قد مكَّنتْ من إنشاء طرق جديدة تستخدم في حرب المعلومات، إلا أننا نرى أن الطرق القديمة لا تزال مستمرة، بل وستبقى قيد الاستخدام إلى ما شاء الله. وسيبقى الجواسيس قادرين على اختراق صفوف الأعداء ومؤسساتهم المختلفة لسرقة أسرارهم، وستبقى أجهزة الشرطة والاستخبارات تتابع الجماعات العدوانية التي تخطط ضد الدول، وسينخرط أفراد من الاستخبارات في صفوف المناوئين لاكتشاف خططهم وأسرارهم. وستبقى الوحدات العسكرية تستخدم المراقبة البصرية إلى جانب أجهزة المراقبة والتحسس البالغة الحساسية وغير ذلك من المعدات والأجهزة للحصول على معلومات عن أرض المعركة. وسيحاول الجميع الانخراط في محاولات تخدع العدو ويقومون أيضاً بحرب معنوية نفسية ضد أعدائهم للتأثير على سلوك أفراد العدو. كما سيستمر الطرفان باستخدام القنابل والقذائف ومختلف أنواع الأسلحة الأخرى للقضاء على أنظمة اتصالات العدو (Denning, 2000b).

ويعتقد أن إدارة الإدراك للحرب النفسية والمعنوية ضد الأعداء ستستمر في لعب دور هام في العمليات المستقبلية. ويتوقع جون بيترسن أن حرب المعلومات في المستقبل ستبدو وكأنها حملات إعلانية تحاول إقناع الأفراد أن يتصرفوا بطريقة معينة تحقق أهداف المحاربين. وستبتعد حرب المعلومات من الأجهزة والعتاد وتقترب من الأفكار والمفاهيم. وستتطلب حرب المعلومات في المستقبل أفكاراً كبيرة وقوية مثل التهديد بالحرب النووية العالمية التي تدفع الناس إلى القيام بعمل محدد، وكذلك التحكم بالأفكار والمعتقدات من خلال الإسقاطات النفسية. ولقد تأثر الفكر البشري

عبر التاريخ بالمعتقدات والأديان، وبالتالي فإن توقعات بيترسن يمكن اعتبارها استمراراً لطرق أزلية قديمة (Petersen, 1996).

إذن، إن ما جلبته التقنية الحديثة هو مزيد من الخيارات والفرص لإجراء حروب معلومات. فهناك المزيد من الوسائل التي يمكن استغلالها في عمليات التخريب، وإلحاق الأضرار والأذى المتعمد والحرب النفسية. وهناك المزيد من مختلف أنواع مصادر المعلومات التي يمكن مهاجمتها، وهناك المزيد من الأدوات التي يمن استخدامها لتنفيذ هجمات قاتلة على مصادر المعلومات. ومن الملاحظ أيضاً أن هناك ازدياداً في نسبة الاعتماد على التقنية في المجتمع، وتزداد بهذا إمكانية احتمالات حدوث خسائر من الهجمات التقنية. وهناك الأدوات الجديدة المؤتمتة الآلية التي يمكن استخدامها في الدفاع أيضاً، ولكن نادراً ما يكون الدفاع عملية ناجحة تماماً، وغالباً ما تتأخر تقنية الدفاع عن تقنية الهجوم. وغالباً ما يجد الغزاة والمتسللون طرقاً ملتوية لتجاوز منافذ الدخول والجدران النارية الدفاعية. إن هناك أسلوب "تجاوز التشفير"، بمخادعة العاملين في داخل المؤسسات بإعطائهم إمكانية للدخول إلى أنظمة المعلومات. ويقوم الغزاة بإطلاق هجماتهم من أمكنة لا يتوقعها متوقع على الإطلاق ولا يدري لها سراً أو سبباً. كما أن السباق بين الهجوم والدفاع لا ينتهي على الإطلاق.

والسؤال الكبير الذي تطرحه داينِنج هنا: هل يستطيع أحد أن يطلق هجوماً كارثيَّ النتائج، وإذا كان ذلك كذلك، فما هي احتمالات حدوث مثل هذا الهجوم؟ والحق يقال: لا يستطيع أحد الجزم بذلك. ومن السهل أن يعد الإنسان عدداً من السيناريوهات مثل: "تعطل سوق الأسهم المالية بعد عبث أحد المتسللين المخربين بأجهزة كمبيوتر وول ستريت"، أو: "اصطدام طائرتين بعد أن قام أحد المخربين بالتسلل إلى نظام التوجيه الجوي وتغيير الطرق والمسارات الجوية للطائرات". ومن الصعب جداً تقدير إمكانية حدوث مثل هذه السيناريوهات أو تنفيذها. ويجب أخذ عدد من العوامل بعين الاعتبار بما في ذلك نقاط الضعف الممكنة في التقنية والطرق التي يمكن استخدام التقنية بها، والإمكانيات اللازمة لاستغلال نقاط الضعف الموجودة في التقنية، والأمور المكررة في التقنية وغير ذلك من عوامل الأمن التي يمكن أن تشكل نقاط ضعف بالنسبة للتقنية، وما إذا كان هناك أفراد لديهم النية أو الرغبة بالقيام بمثل هذه الأعمال العدوانية الشريرة المدمرة، والفرصة لتنفيذ هجماتهم المطلوبة (Denning, 2000 b).

المبادئ الجديدة للحرب في عصر المعلومات

يذكر ليونهارد (Leonhard, 1998) (ص 251-261) أن الصراع البشري يقوم على ثلاثة قوانين هي (1) القانون البشري، و(2) القانون الاقتصادي، و(3) قانون الازدواجية. يعد القانون البشري هو الأساس ويقوم عليه القانونان الآخران. والشكل التالي يبين العلاقة بين هذه القوانين والمبادئ التي تمثلها، وفيما يلي استعراض لهذه المبادئ:

شكل رقم (3) مبادئ الحرب في عصر المعلومات.

المصدر: شكل 16-1 (Leonhard, 1998, p.252).

مبدأ المعرفة والتجاهل

تتعلق المعرفة (Knowledge) بما نعرفه من معلومات أو ما ننوي معرفته عن أنفسنا أو عن أعدائنا أو عن البيئة. أما التجاهل (Ignorance) فهي عكس المعرفة، وتتعلق بما لا نعرفه وبما لا نستطيع معرفته أو بما نختار أن لا نعرفه. ولقد سيطرت كلا من المعرفة والتجاهل على الحرب عبر تاريخها، ولكن حرب المعلومات قد عدلت الميزان تجاه المعرفة.

إن إحدى مهارات الفعاليات لما نعرفه وما لا نعرفه. إن مبدأ ال ى فرض فإن القائد يمكن أن يعرف عين. و فإن عليه أن يختار أن لا يركز نت لذلك التجاهل. إن جوهر المهارة في عصر المعلومات هو إدارة ما نعرف وما لا نعرف، والموازنة بين معرفتنا فيما يتعلق ب بدأ المعرفة والتجاهل مشروط بقانون الاقتصاد. إن جاهل لا تعني إن المعرفة شيء جيد والتجاهل يجب تجنبه، ولكن يجب أن نعرف أن للمعلومات كلفة مرتبطة بها الحقيقة في أرض المعركة تكلف الوقت والمال، والأرواح والمعدات، والتجاهل بلا كلفة.

القانون البشري

قانون الازدواجية

القانون الاقتصادي

المعرفة والتجاهل

مبادئ السيطرة

مبادئ التفاعل

مبادئ الاقتصاد

إن القانون الاقتصادي يسعى إلى تقليل الكلفة، والكلفة ذات جوانب متعددة: المال والمعدات والوقت والحياة. وقد نختار الجهالة (الإهمال) وهي رخيصة وجاهزة. وإذا كان الخيار للجهالة (الإهمال)، ففي هذه الحالة فإن بقية جوانب الحرب ستكون مكلفة. فإننا سندفع أضعاف في مجالات الحرب، وهي تعتمد على مواقف العدو وليس على قصده، وهي تستجيب للعدو أكثر من أها

التحييد والمواجهة

الفرصة وردة الفعل

خيار السريع والهدف

التوزيع والتركيز

فاعلية الأمن

السيطرة والفوضى

أما الخيار الآخر فهو المعرفة ية ذلك أنها توجد فقط كنظام للنظم (System of Systems). إن السيطرة المعلوماتية تعتمد على الحاسب، والاتصالات، وتقنية الاستشعار والتدريب المبتكر معاً وأكثر. إن الاستثمار متغير الأجل في المعرفة يؤدي إلى اقتصاد قوي في كل جانب من جوانب

مبادئ السيطرة

تطرح مبادئ السيطرة كيف تدير القوة الصديقة،ن وتقدم مبدأ السيطرة التي تستخدم على قواتنا ذا تأثير على فرص نجاحها في الصراع مع العدو.

1- **مباديء تسريع البديل والهدف** (Option Accelaration & Objective)

يقوم مبدأ تسريع البديل على تأخير القرار الخاص بالهدف المرغوب للصراع، والتركيز على المرونة لتحقيق أكبر مخرجات ممكنة. وبالتالي يعمل القائد العسكري على استخدام القوة العسكرية لتحقيق بدائل تكتيكية وعملياته واستراتيجية لتعطيل خطط العدو وردود فعله والتي تقلل من خطط العدو وردات فعله. إن ميزات تسريع الخيار يتمثل في سرعة في رد الفعل، والقدرة على استغلال الفرص غير الظاهرة. أما الهدف فيسعى إلى تكوين قرار مبكر يتعلق بالهدف المرغوب للصراع وبعدها العمل على القرار من خلال حملة سريعة ومركزة. ويوحد المفهوم العلمي من خلال اختيار أهداف مسبقة وقابلة للتحقيق قبل العمليات القتالية.

ويظهر مبدأ المعرفة والتجاهل في تطبيقات هذا المبدأ، فكلما زادت المعرفة كلما كانت السلطة مثالية (سواء كانت حكومية على المستوى الاستراتيجي، أو العسكري التكتيكي، أو مستوى العمليات الحربية) كلما كانت فرصة أكبر لتسريع الخيار. والعكس كلما زاد التجاهل كلما كانت السلطة مثالية، كلما زاد اعتمادها على الهدف.

2- **مباديء السيطرة والفوضى** (Command and Anarchy)

السيطرة هي الممارسة القانونية والإجرائية للسلطة على المرؤوسين، أما الفوضى فتؤدي إلى توليف النشاطات لوحدة ما. وعلى الجانب الآخر المتطرف من مبدأ السيطرة نجد هرمية محددة مؤسسة مع قبول القواعد والممارسات. أما الجانب الآخر من مبدأ الفوضى نجد أشياء متساوية/ تابعة بلا روابط/ قانونية أو اجرائية.

يتطلب مبدأ السيطرة مبدأ من خلال توجيه السلطة وينزع أن يستفيد من فعالية التحكم، وينزع لفقد الفعالية في التفاعل مع العدو، أما جانب السيطرة من هذا المبدأ فيؤدي إلى وضع قرار سريع واقتصادي، ولكنه يعاني من وضع ضغوطات غير اقتصادية على نشاطات المرؤوسين.

أما مبدأ الفوضى فيسعى إلى النجاح من خلال التكامل الماهر للآثار. الفوضى تنزع إلى الحصول على التفاعل مع العدو، ولكنها تفقد الفاعلية في عمليات التحكم، وهي تقود إلى استثمار اقتصادي عالي لنشاطات المرؤوسين ولكنها تعاني من صنع قرارات غير اقتصادية.

ويشترط مبدأ المعرفة والجهالة تطبيق السيطرة والفوضى، كلما زادت المعرفة للمسؤولية في القيادة كلما زاد ويجب أن تطبق الأوامر بفاعلية، كلما زادت الجهالة للقادة كلما زادت إمكانية استخدام الفوضى بفعالية.

مجالات حرب المعلومات

وصفت داينبنج (Denning, 2000 b) هذه المجالات بأنها تتراوح بين ساحات اللعب (Playgrounds) إلى ارض المعارك (Battlegrounds). وتعد حرب المعلومات نشاطاً يتم في سياق الفعل والصراع الإنساني، وتلخص داينبنج (Denning, 2000 b, p. 43) نشاطات حرب المعلومات في أربعة مجالات رئيسة هي :

أ ـ العبث (اللعب) (Play).

ب ـ الجريمة (Crime).

ج ـ حقوق الفرد (Individual rights).

د ـ الأمن الوطني (National Security).

أ ـ العبث (اللعب) (Play)

ويتعلق مجال اللعب بخرق نظم المعلومات لغايات التسلية والتحدي، في حين يتعلق مجال الجريمة بالسلوكيات غير القانونية المتعلقة بجرائم الملكية والاحتيال بالحاسب وسوء استخدامه، وتمثل الصراع بين الضحايا والفاعلين للجريمة. أما مجال حقوق الفرد فتغطي الصراعات في مجال حرية التعبير والكلام والخصوصية وهذا يظهر بين الأفراد ، والمنظمات أو الحكومات، وأخيراً مجال الأمن الوطني والذي يتعلق بالصراع على المستوى الوطني ويشمل عمليات التجسس الأجنبية والحروب والصراعات العسكرية والعمليات ضد الدولة من خلال لاعبين غير الدول، وهذه المجالات متصلة. فمجال اللعب يُعد جريمة من مثل خرق قواعد بيانات مؤسسة

حكومية أو تدميرها أو تخريبها، كل هذه سلوكيات جرمية. إن خرق نظام حاسب ما، أو سرقة رقم بطاقة ائتمان من خلال الاتصال بالانترنت أو تجسس تجاري كله يؤدي إلى انهيار نظام الحاسب، وبالتالي فإن التمييز بين هذه المجالات الأربعة عملية صعبة وفيما يلي أهم الفئات في هذه المجموعة.

الدخلاء .(Hackers). الدخلاء أذكياء، مبدعون (Levy, 1984) الدخول غير الشرعي وغير القانوني للحاسب بقصد المتعة، أو العبث، أو الإجرام. ويعد الدخلاء أطفالاً أذكياء، ولكن بعدما تغيرت الأوضاع فيما يخص التمكن من الدخول غير المسموح به (قانونياً أو أخلاقيا) إلى الشبكات وقواعد المعلومات والحاسبات . . . إلخ، إصبح المفهوم يعني وصماً لهذه الفئة وليس لمن يستخدم الحاسب كهواية ويستمتع بالتعلم منه. يعني مصطلح الدخلاء من يتمكن خرق نظم الحاسب (الحصول على دخول غير مصرح به). ويتصف الدخلاء في فترة الثمانينات والتسعينات بما يلي: ذكي، متحمس للحاسب، منطوي، وغير آمن، من طبقة متوسطة إلى أعلى المتوسطة. أما دوافعهم فتتراوح بين التعلم من الحاسب كهواية، وهزم السلطة، والاستجابة للتحدي، والتغلب على النظام، والتسبب بالإرباك للآخرين، وإظهار الذكاء والتحدي. هناك ثلاثة أنواع من الدخلاء هم :

1- الفضولي (Curious) الذي يخرق نظام الحاسب إلى الحاسب أو الشبكة ليتعلم عنه أكثر.
2- الجانح (Meddlers) وهو الذي يتدخل فيما لا يعنيه، وهو الذي يخرق نظام الحاسب أو الشبكة لأنه مهتم به وفي الاستجابة للتحدي ويبحث عن نقاط الضعف في النظام.
3- المجرم (Criminal) والذي يخرق نظام الحاسب أو الشبكة لارتكاب جريمة للحصول على منفعة ذاتية. (Levy, 1984, Kovackch, 1993).

الدخيل الفضولي (The Curious Hacker). هناك اتفاق على أن أول الدخلاء غير المصرح لهم من هذا النوع كانوا من معهد ماساتشوسس للتكنولوجيا (MIT) في الخمسينيات والستينيات، وكانت المجموعة تنتمي إلى نادي (MIT) والمعروف بنادي أنموذج السكة الحديدية (TMRC). وفضولهم قادهم إلى التساؤل عن الكيفية التي تعمل بها الأشياء، وكيف يمكن أن تعمل بشكل أفضل، هؤلاء الدخلاء يستمتعون

بالتعلم عن الحاسب وعن الكيفية التي يمكن أن تتوسع بها امكانيات الحاسب. ولقد بدأوا بتطوير مصطلحاتهم الخاصة بهم من مثل الخسارة (Losing). أما مصطلح الدخيل فقد استخدم سابقاً في معهد الـ (MIT) لتعني مبرمج الحاسب الذكي المبدع، والفسلفة هي المشاركة والانفتاح، واللامركزية، والتعامل مع الآلة بغض النظر عن أي كلفة لتحسينها وتحسين العالم. وهم يعتقدون أن المعلومات يجب أن تكون مجاناً، إنهم لا يثقون بالسلطة، وأنه يجب أن ينظر إليهم في ضوء قدراتهم ومهاراتهم. (Steele; Woods; Finkel; Grispin; Stallman, and Goodfellow, 1983).

الجانح (The Meddler) الجيل الثاني من الدخلاء حمل روح الدخلاء الأوائل ولكن بنشاط أكثر في خرق نظم الحاسب. والجانح (الدخيل) هنا هو فضولي، وتشكل محتويات الحاسب و نظامه اغراءً له ويحاول خرقها، ويحاول الحصول على كلمة المرور، ورقم الهاتف، والبرامج اللازمة، وعند الحصول عليها يحاول الدخول للنظام.

أما الدخلاء الجانحون فيدخلون إلى النظام لأنهم مهتمون بالتحدي في خرق النظام والبحث عن الثغرات فيه، ففي السابق كانوا يستخدمون برمجيات معينة تحدد الهاتف الذي يعمل مع الإنترنت ويحاولون الوصول إلى اسم المستخدم وكلمة المرور (Password) ليتمكنوا من الوصول إلى نظام الحاسب، واليوم يستخدمون محركات البحث مثل ياهو (Yahoo)، وليكوس (Lycos)، واكسايت (Excite) للبحث عن أدوات دخول ولم تتوقف أعمال الدخلاء الجانحين اليوم على التحدى بل شملت تدمير المعلومات وأغلاق النظام.

وهناك برامج متوفرة الآن على الإنترنت ومجاناً يمكن الاستعانة بها لهذه الأعمال، وهؤلاء يدخلون إلى النظام بقصد التحدي واكتشاف ما عليه، وكيف يعمل وعادة يتعلمون أكبر كمية ممكنة عنه. وهم يحددون ثغرات الدخول للنظام ويقدمون النصح للقائمين عليه لسدها. وليس لديهم النية في التخريب والفرق بينهم وبين النوع السابق أنهم يدخلون إلى النظام دون موافقة أو تصريح، وإذا ما حدث تحد لهم يصبحون أحداثاً منحرفين.

يدخل المجرمون إلى نظام الحاسب لارتكاب جريمة، وللحصول على منفعة شخصية وتدمير المعلومات، أو سرقتها، أو تدمير ملفات النظام أو الابتزاز ببيع المعلومات لأطراف أخرى. وهناك نوعان جديدان من الدخلاء هما الدخلاء الدوليون (International Hackers) وهم الذين بدأوا الدخول للنظم الأمريكية من أوروبا،

وهناك الـ(KGB) التي قيل انها دفعت إلى الدخلاء لخرق الحاسبات الأمريكية. أما النوع الآخر فهم الذين يخرق نظم التلفونات والمعروف باسم (Phreakers).

دخلاء التلفون (The Phreakers) : يُعنى دخلاء التلفون باختراق نظم التلفون وإجراء مكالمات حول العالم دون دفع قيمتها، ومن المعروفين كأوائل في هذا النوع من التعدي كابتن كرنشي (Captain Crunch) والذي تمكن من إجراء مكالمات دولية مجاناً بخرقه نظام الهاتف، وهناك شخص آخر عرف باسم الكرايكر (The Cracker) ومارس هذا السلوك منذ عمر (14) سنة (Landreth, 1985).

2- المتسللون (Crackers):

المتسللون أشخاص يخرقون الإجراءات الأمنية لنظام الحاسب والحصول على دخول غير مصرح به، والهدف قد يكون الحصول على معلومات بطريقة غير قانونية من الحاسب أو استخدام مصادر الحاسب.

في أي من المجموعات الثلاث السابقة يمكن أن يوصف الفعل بأنه نوع من التسلل أو القرضة، والقراصنة جماعة فريدة، وتاريخياً فقد كان الحافز بوصفهم متحدين وهم يعملون في جماعات أو بشكل فردي، ولكن غالبيتهم يعملون بشكل فردي. وتنزع جماعة المتسللين إلى أن تكون غير رسمية، ولقد كان أول مؤتمر للقرصنة الدولية المنظمة في عام 1990م، في أوروبا حيث اجتمع فيه القراصنة من كافة أنحاء العالم لتبادل الآراء والتعلم في الدخول إلى أنظمة الحاسب والممارسة . . . إلخ.

3- العابثون (Vandals) :

إن فئة العابثين (الذين يتعدون على الملكيات العامة أو الخاصة) لا يرتكبون جرائمهم للإثارة العقلية (كما في حال الدخلاء والمتسللون) أو المكسب المادي أو السياسي (مثل مجرمي الحاسب). فغالبية هذه الفئة غاضبة من مكان عملهم أو من الحياة بشكل عام. ويمكن تقسيمهم إلى مجموعتين :

1- المستخدمون (Users) الذين لهم حق استخدام النظام يتعاملون مع النظام الذي يخترقونه أو يسيئون استخدامه.

2- الغرباء (Strangers) الذين ليس لهم حق استخدام النظام.

إن الدخول للنظام أو خرق نظام الحاسب ليس دائماً غير قانوني فأصحاب القبعات البيضاء (White Hats) يقومون بخرق النظام بناءً على الطلب من أشخاص لمعرفة مدى قدرته على الحماية. أما أصحاب القبعات السوداء (Black Hats) فهم الذين يخرقون نظم الآخرين دون أذن وغالباً لغايات مادية. أما الأسباب لذلك فمتعددة منها التحدي للنظم السائدة، أو للمتعة بخرق النظام، أو الدخول بالقوة، أو لأجل المعرفة، أو لأجل الحصول على الاعتراف والتقدير.

ب ـ الجريمة (Crime):

المجال الثاني لحرب المعلومات هو الجريمة، ويمكن تصنيف السلوكيات على أنها جرائم في الفئات التالية :

1 ـ **جرائم الملكية الفكرية** (Intellectual Property Crimes) : تشمل جرائم الملكية الفكرية نسخ البرامج غير القانوني (Piracy) والسرقة والاتجار بالأسرار التجارية. كما تشمل جرائم النسخ غير القانوني للمعلومات أو حيازة المعلومات بطريقة غير قانونية وتوزيع المواد ذات حقوق النشر بما في ذلك الصور في الصيغة الالكترونية والمطبوعة، والمواد المرئية والسمعية والمخزنة على شرائط أو أقراص مرنة أو أقراص مدمجة أو على الحاسب . . . إلخ. لقد قدرت خسارة شركات المعلومات الرئيسة في الولايات المتحدة عام 1996 بين 18-20 مليار دولار بسبب النسخ غير القانوني خارج الولايات المتحدة. وتؤكد تقارير الدراسات المسحية مثل (SIS) أن غالبية مجرمي المعلومات المتعلقة بجرائم الملكية الفكرية هم من الموظفين السابقين والحاليين والمؤقتين أو الموردين أو المستشارين (ASIS, 1996).

2 ـ **الاحتيال** (Fraud) : تشمل الجرائم في هذه الفئة احتيال التسويق (Telemarketing Scams)، وسرقة الهوية، والاحتيال على البنوك، والاحتيال في الاتصالات، والاحتيال في الحاسب وسوء استخدامه. وبشكل عام فإن أي فعل احتيال ربما يعد حرب معلومات إذا استغل مصدر معلومات إلى صالح فريق آخر وضد آخر. ويشمل الاحتيال من نوع (Telemarketing) الحصول على معلومات عن الأشخاص من خلال التلفون، أو البريد، أو البريد الإلكتروني، أو الإنترنت، وتقديم عروض وهمية.

أما الاحتيال في مجال الهوية (Identity) فيشمل الحصول على الدخول إلى هوية شخص آخر من مثل الاسم، الرقم الوطني، رخصة السواقة، أو بطاقة الائتمان . . . إلخ. وهناك حالات احتيال كثيرة منها (Vladimir Levin) وهو موظف حاسب في (St. Petersburg) اتهم بمحاولة سرقة (10) ملايين من حسابات أحدى الشركات الكبرى.

وفي مجال الاحتيال في الاتصالات فإن المجرمين يحصلون على خدمات الهاتف ويبيعونها، انهم يختلسون السمع (Eavesdroper) على الاتصالات اللاسلكية ويلتقطون أرقام الهواتف وبرمجياتها ويحولونها إلى هواتف مستنسخة (مقلدة) (Cloned) والتي ترسل الفاتورة إلى الضحية. وقدرت الخسارة للهواتف اللاسلكية في الولايات المتحدة عام 1966م بمليار دولار، أما الخسارة في عام 1992م لهذا النشاط فقدرت (8.9) مليار دولار.

3ـ سرقة الأرصدة (Theft of Assets) :

إن البنوك تخسر مبالغ كبيرة قدرت في بريطانيا بمبلغ (2.7) بليون باوند سنوياً نتيجة الاحتيال المالي وسوء الاستخدام لبطاقات التسليف (Visa Card)، وهذه من الطرق التقليدية في التعامل المالي. إن المؤسسات المالية ضحية للاحتيال المالي ليس بسبب الانترنت، وإنما بطرق أخرى، ففي بداية 1995م، أظهرت نتائج دراسة ماستر كارد (Master Card) المسحية أن (66٪) من المستجيبين قد استخدموا الـWeb للإطلاع على البضائع وأن (28٪) منهم قد اشترى عن طريقها، في حين رأى (58٪) منهم أن الانترنت قناة مهمة في الاطلاع والاختيار من المواد المعروضة، والخلاصة هي أن الأفراد قد قبلوا الانترنت كمكان آمن لممارسة أنشطتهم الاقتصادية (Watson, 1997, p. 52). وتم سرقة مليارات الدولارات من خلال التحويل الإلكتروني أو من البنوك أو الأسهم.

4 ـ سرقة البرامج (Theft of Sofware) :

ويقصد بها سرقة البرمجيات التطبيقية سواء كانت تجارية أو علمية أو عسكرية . . . إلخ. حيث تمثل هذه البرمجيات جهوداً تراكمية لسنوات من نتائج التطوير والبحث، وهي ذات قيمة مادية كبيرة جداً، وبالتالي فهي تمثل قيمة مادية ومعنوية كبيرة جداً مما يجعلها تشكل اغراءً للآخرين لسرقتها.

5- التدمير (التخريب) بالحاسب (Sabotage by Computer) :

التدمير بواسطة الحاسب لشبكات الحاسب، أو للمعارف . . . إلخ. فالعبث في أجهزة الحاسب التي يعتمد عليها الأفراد أو المنظمات في أعمال معينة تشكل أعمالاً تخريبية، ففي عام 1995م، تم إيقاف الحاسبات التي تنظم حياة مجموعة من المرضى في مستشفى جيس (Guyis Hospital) في لندن، أو وضع فيروس في حاسب شركة ما، أو ما يسمى بقنابل البريدية . . . إلخ. (Icove, Segert & Vonstorch, 1995). ويشمل التخريب إتلاف المعلومات، أو تعطيل الحاسب (IFS, 1998)، أو مسح البيانات أو تشويهها .

6- إعادة نسخ البرامج :

شكل التعدي على الملكية من خلال إعادة نسخ البرامج مشكلة بين الولايات المتحدة والصين ودول النمور الآسيوية، حيث لا توجد قوانين تمنع ذلك، إلا أن مثل هذا النسخ غير المشروع يؤدي إلى خسارة كبيرة للشركة الأم وأرباح طائلة للناسخين. وقد تبين أن ما يقارب من (2) مليار دولار أمريكي هي الخسائر الناتجة عن سرقة برامج الحاسب الآلي عبر شبكة الإنترنت عام 1997 (Intergov, 1999).

7ـ التجسس :

تشكل المعلومات ثروة وقوة في المجتمع المعلوماتي، حيث يمكن للمنافسين من الشركات والدول انفاق مبالغ كبيرة في سبيل الحصول على معلومات تقنية عالية أو أسرار عسكرية أو سياسية أو تجارية . . . إلخ. ومثال على ذلك ما أُشيع عن تجسس الصين على مختبرات الأسلحة الأمريكية والتي أدت إلى أزمة بين البلدين. ويعنى التجسس الحصول على معلومات هامة من الناحية الإستراتيجية، أو العسكرية، أو التقنية، أو التجارية، أو معلومات ذات طبيعة سرية (Davis, 1998)، وقد يكون التجسس عن بعد أو من داخل الموقع (Vacca, 1996).

8- التخريب الإلكتروني:

ويمتاز هذا النوع من التخريب بأنه يتعمد المعلومات والبيانات الموجودة على الحاسب وفي غالبية الأحيان يتم عن بعد، وقد تستخدم في هذه العمليات ما يسمى

بالقنابل الإلكترونية، وهي رسائل مفخخة يمكن إرسالها للشبكات المستهدفة وتدميرها. وقد تستخدم طرق التخريب عبر شبكة الإنترنت من قبل قراصنة الحاسب أو الجماعات ذات الأهداف الخاصة، من مثل أولئك الذين احتجوا على الانتشار النووي، وقد كانت الساعة الأولى من تاريخ 26 أبريل 1999م، هي ساعة الصفر لهذا الفيروس، وقد اختير هذا التاريخ مواكباً لذكرى انفجار ذلك المفاعل النووي، هادفة تلك الجماعة التخريبية من ذلك لفت انتباه العالم لتلك الذكرى (العامر، 1999م).

وفيروس الحاسب يشبه في عمله الفيروس الذي يصيب الإنسان، حيث إنه برنامج يصممه بعض المخربين وله القدرة على ربط نفسه ببرامج التطبيقات أو نظم التشغيل ثم يتكاثر وينتشر داخل النظام حتى يتسبب في تدميره تماماً، وتمتاز الفيروسات :

أ ـ مخفية (أي أن المستخدم لا يعرف عنه) إلا إذا استخدم برامج كشف الفيروسات، إلا أن اعراضه قد تمكن من الكشف عنه من مثل البطء في عمل الحاسب وعدم فتح الملفات أو تغير في أشكالها، وغالباً ما يكون في هيئة ملفات مخفية في نظام الحاسب الآلي (Hiden Files) بحيث لا يستطيع مستخدم الحاسب الآلي ملاحظة وجودها بالطرق العادية. وبعضها يوجد في ذاكرة الحاسب الآلي ويكون مرتبطاً بتاريخ أو ساعة جهاز الحاسب الآلي. حيث يكون مبرمج على العمل التدميري لبيانات الحاسب في وقت وتاريخ معين (خليل، 1994).

ب ـ سرعة الانتشار : مثلما أن الإنترنت قد قدمت خدمات جليلة وهامة للإنسانية إلا أن استخداماتها السلبية لا زالت تشكل تهديداً كبيراً على مستوى العالم. حيث إن وضع فيروس حاسب ما عليها يمكن أن ينتشر بسرعة لدى دول العالم. مما يؤدي إلى خسائر كبيرة (خليل، 1994)، مثل فيروس الحب.

ج ـ الاختراق : إن لبعض الفيروسات القدرة على اختراق الموانع الأمنية في بعض أنظمة الحاسب ليعمل على تدمير البيانات الموجودة على ذلك الحاسب، أو إعطاء أوامر ضارة لمكونات الحاسب الآلي تؤدي إلى تلفه (خليل، 1994).

د ـ التدمير: بعض فيروسات الحاسب تؤدي إلى تدمير محتويات الحاسب من البرامج والمعلومات وبيانات والبعض الآخر يعمل عند تشغيل الحاسب (IFS, 1998)

9- التحريف :

وهو التلاعب بالمعلومات المخزنة في أجهزة الحاسب المرتبطة بشبكة الإنترنت أو اعتراض المعلومات بين أجهزة الحاسب عبر الشبكة ويشمل تحريف البيانات اعطاء أسماء وهمية مثلاً أو تغير الأسماء أو المعلومات المتوافرة في الحاسب (الصغير، 1992).

10- السرقة :

لم تعد سرقة أجهزة الحاسب الآلي بعينها تمثل أهمية لصاحبها بقد ما تمثله المعلومات والبرامج المخزنة فيها من أهمية (Orlowski, 1998)، وتتمثل السرقة في اختراق الشبكات أو أجهزة الحاسب، وقد يشمل ذلك تحويلات مصرفية غير مشروعة عن طريق اختراق شبكات المصارف المالية والبنوك، وهناك الكثير من الحالات التي تم فيها تحويل مبالغ مالية كبيرة من حسابات إلى حسابات أخرى أو اعتراض عمليات مالية من خلال التحويل.

ج ـ حقوق الفرد (Individual Rights)

إن الصراعات بين الأفراد خاصة في مجال الخصوصية وحرية التعبير، وهذه الصراعات بين الأفراد ـ الأفراد، والأفراد ـ المؤسسات، والأفراد ـ الحكومة، ومن الأمثلة أن فرد تشوه سمعته (Defaming) أمام العامة أو على الإنترنت، والهدف تلويث سمعة أو شخصية الفرد، ومن الأمثلة الأخرى ما يسمى حرق الشخصية (Flaming) (اغتيال شخصية وتحريض للآخرين)، أو إرسال رسائل تهديد، أو رسائل التحرش، أو تفجير صندوق بريد الكتروني يحتوى على ملايين الرسائل، أو التجسس على الآخرين، أو التنصت على المكالمات، أو كشف معلومات سرية حول طرف ما. هناك الكثير من المجالات المتعلقة بالصراع محمية بالقانون إلا أن هناك مجالات أخرى غير محمية.

وتشمل حرب المعلومات في مجال الصراعات من الأفراد ومؤسسات الأعمال سرقة الملكية الفكرية وتوزيعها. وكذلك فإن الحكومات تمارس درجات من الضبط على وسائل الإعلام والمطبوعات وهي تحرم بعض أنواع الكلام وفي ذلك حرمان للمواطن من أنواع معينة من المعلومات وهذه كلها تأتي تحت الرقابة (Censorship)

لحماية المصالح الوطنية. وفي بعض الدول كالولايات المتحدة فإن مراقبة المواطن لا تكون إلا بأمر من المحكمة بناء على سبب محتمل لنشاط جرمي. وبعد أحداث (9/11) فقد سمح للأجهزة الأمنية الامريكية من التجسس على البريد الالكتروني والانترنت لغايات مواجهة الارهاب. وهو ما عرف بقانون باتريوت.

د. الأمن الوطني

ويشمل هذا المجال العمليات التي تقوم بها الدول الأخرى أو الأفراد ضد الدولة ومنها عمليات الاستخبارات الأجنبية، والعلميات العسكرية والحروب، الإرهاب، وحرب الشبكات (Netwar). وفي كلمة أمام أعضاء وكالة المخابرات المركزية الأمريكية (CIA) حدد الرئيس كلنتون (Clinton) أولويات لجنة الاستخبارات الأمريكية بـ :

1- الحاجات الاستخبارية للجيش خلال العلميات.

2- الاستخبارات العسكرية والسياسية والاقتصادية عن الدول المعادية للولايات المتحدة والمعلومات عن التسلح والاقتصاد والسياسة للدول المحتملة عدائيتها للولايات المتحدة.

3- الاستخبارات عن تهديدات محتملة مثل الإرهاب والمخدرات والسلاح والجريمة المنظمة والممارسات غير القانونية والبيئة. . . إلخ. (Denning, 2000b, p. 63).

أما اليابان فكانت سياسة مخابراتها في الثمانينات تتمحور حول الحصول على المواد الخام، والتطورات التقنية والعملية في الولايات المتحدة وأوروبا والوصول لصانعي القرار السياسي في الولايات المتحدة وأوروبا خاصة في مجال التجارة والمال والسياسة العسكرية في آسيا ومناطق الباسفيكي والتطورات العسكرية في الاتحاد السوفيتي والصين وكوريا الشمالية. وملخصها كما قال بن فنزك (Ben Venzke) مؤلف (التقرير الاستخباري في اليابان، فإن الفلسفة هي لماذا نقضي (10) سنوات وندفع (1) مليار دولار في البحث والتطوير بينما نستطيع أن نرشي مهندس منافس (1) مليون ونحصل على ما نريد إن لم يكن أفضل مما نريد) (Petersen, 1996).

ظهر في تقرير لـ (Defense Investigative Service) و(FBI) أن الأهداف مكان التجسس في الولايات المتحدة هي التقنية العالية، والصناعات العسكرية، حيث إن

امتلاك هذه التقنيات يمكن الدول من تطوير نظم أسلحة ذات فعالية مواد أخرى دون الإنفاق المادي الكبير في مجال البحث والتطوير. ومن مجال التجسس في هذا المجال البيوتكنولوجي والنظم الكميائية والبيولوجية، والحاسبات، ونظم المعلومات والاتصالات، وحرب المعلومات، والمجسات والليزر، والإلكترونيات، وأشباه المواصلات، والصناعة، والطاقة، والنظم النووية، والفضاء، ونظم البحرية، والأسلحة. ومن أهم مواضيع التجسس على الولايات المتحدة كانت في المجال التجاري في عام 1998م كان هناك (800) حالة رسمية. وقد قدرت الـ (FBI) خسارة الولايات المتحدة في الأعمال من قبل الدول الأجنبية بـ(100) مليار دولار. إن ما تنفقه الولايات المتحدة على البحث والتطوير (249) مليار هو ما جعلها قوية اقتصادياً.

ب ـ **الحرب والصراعات العسكرية** : لقد أدخل اركويلا (Arquilla)، ورونفلديت (Ronfeldt) مفهوم حرب المعلومات الفضائية (Cyberwar) في مقالتهما حرب الفضاء قادمة، وهذه الحرب قائمة على التخريب والتدمير للمعلومات، أو تعطيلها لتنفيذ عمليات عسكرية معينة، وتوظيف التقنية الحديثة مثل الحاسب، والشبكات، والتشفير، وفك التشفير كأدوات في هذه الحروب.

في عصر المعلومات تغيرت مفاهيم الصراع والحرب، فحل هواة الحاسب، وقراصنته، والمتسللون والمتطفلون والدخلاء، وحتى الأطفال محل الجنود. هل ستكون حرب المعلومات حرباً بلا دماء، حرباً بلا جيوش ؟ إن تدمير البناء التحتي المعلوماتي للمجتمع يحوله إلى مجتمع أعمى، وأصم، وأبكم، تفقد السيطرة والتحكم فيه بين أجزائه المختلفة. إن تعطل النظم المدنية ونظم الطاقة والمياه، والهاتف، والبنوك، والمال، والاتصال، والطيران . . . إلخ. سيحول المجتمع إلى حالة أنومي معلوماتية (Anomie) تفسخ معلوماتي يؤدي إلى شلل، وتعطيل بوظائف المجتمع كله، مما يسهل السيطرة عليه، وتصبح الجريمة عملية سهلة. إن تدمير الشبكات المعلوماتية، وتغذية نظم معلومات العدو بمعلومات خاطئة تعجل بالنصر للطرف الآخر.

ج ـ **الإرهاب** (Terrorism): يرجع الإرهاب إلى التهديد باستخدام العنف أو استخدامه مع نية (تحقير) (Intimidating) أو إجبار المجتمعات أو الحكومات للرضوخ

لمطالب معينة. ويمكن أن يقوم به فرد أو جماعة وغالباً ما يكون مدفوعاً بأهداف ايدولوجية أو سياسية.

وتستخدم المجموعات الإرهابية عمليات التشفير في حفظ معلوماتها، وذكر أن رمزي يوسف المتهم بتفجير المركز التجاري الدولي في نيويورك بالولايات المتحدة الأمريكية عام 1994م، وتفجير طائرة مانيلية قد شفر ملفات محفوظة على حاسبه الشخصي، وعند فك التشفير تبين وجود معلومات تشمل خططاً لتفجير (11) موقعاً أمريكياً يتعلق بمكاتب الطيران في دول مختلفة، وهناك العديد من الحالات تضمنت تعديات فيزيقية على الحاسبات، ونظم الاتصالات، والتعديات بواسطة البرمجيات ذات الوظيفة التدميرية صفة لازمت تعديات الإرهاب المعلوماتي (Information Terrorism) وهذا يشمل الدخول التخريبي وحذف (مسح) الملفات، ونشر فيروس الحاسب عمداً على الشبكة وعلى الإنترنت والتي تؤدي إلى تعطيل الحاسبات عن بعد. وعلى أية حال فإن هذه الأفعال لا تنفذ من قبل الإرهابيين فقط (بمعنى الإرهاب) ويمكن من المتلصصين(Hackers) والموظفين الحاقدين وتستهدف منظمة بعينها (Denning, 2000).

ومن التعديات التي وصفت كإرهاب إلكتروني (Cyberterrorism) ما قام به مقاتلو التاميل (Tamil Guerrillas) عندما أمطروا سفارات سيرلانكا بآلاف الرسائل الإلكترونية، وكانت الرسائل تقول «نحن نمور الإنترنت السود ونقوم بهذا لشل اتصالاتكم» (E-mail attack, 1998). وكانت غارات البريد الإلكتروني تتمثل في إرسال (800) رسالة إلكترونية يومياً لمدة أسبوعين، ولقد ساهم هذا الهجوم في نشر الدعاية عن مقاتلي التاميل.

لقد استخدم باري كولن (Barry Collin) في الثمانينات استخدام مصطلح الإرهاب الفضائي (Cyberterrorism) بأنه اعتداء مدفوع سياساً ضد المعلومات، ونظم الحاسب، وبرامج الحاسب، والبيانات، ويؤدي إلى العنف ضد أهداف سليمة من قبل مجموعات أو عملاء» (Pollitte, 1997, p. 285).

ورسم كولن (Colin) عدداً من الاحتمالات للإرهاب الفضائي منها وصول هجمات إرهابية إلى نظام التحكم في صناعة طعام الأطفال (Cereal) وتغير مستويات

الحديد، مما يؤدي إلى مرض الأطفال ووفاتهم، أو الوصول إلى نظام التحكم في الملاحة الجوية وسقوط طائرة ركاب عملاقة، أو نظام التحويل المالي الدولي . . . إلخ . (Colin, 1997) .

د ـ **حرب الشبكات** (Netwars): لقد قدم اركويلا ورنفلدت (Arquilla & Ronfeldt) مفهوم حرب المعلومات في ثلاثة مستويات هي: (1) حرب الشبكات «وهي المعلومات ذات الصلة بالصراع مع المستوى الكبير بين الأمم أو المجتمعات»، وتشمل تعطيل وإرباك وتدمير البنية التحتية المعلوماتية لدى الخصم. (2) الحرب الفضائية (Cyberwar) يتعلق بالعمليات العسكرية التي تتم وفق المبادئ المتصلة بالمعلومات. ويتعلق بالصراعات المرتبطة بالمعلومات والتي يغلب عليها التوتر المنخفض من فاعلين غير الدولة بما فيها المنظمات غير الحكومية (NGOS). ويتوقعان أن الصراعات المستقبلية ستكون بين المجموعات المنظمة أكثر من الشبكات كهرميات، ويمكن للشبكات أن تهزم المؤسسات، ويصعب على الهرميات مصارعة الشبكات، (3) الارهاب الفضائي (Cyberterrorism) وهذا هو المستوى الاخير من حرب المعلومات. وهو استخدام الارهاب للمعلومات ومهاجمة البناء التحتي المعلوماتي خاصته مع زيادة الانكشافات في هذه البنية. (Arquilla & Ronfeldt, 1996) .

هـ- **تقانة التجسس**: لقد وظفت التقنيات الحديثة في عمل التجسس وأعمال المخابرات والعملاء بشكل كبير، وأصبحت متاحة للمواطن العادي. ولقد استخدمت التقنيات في التجسس بشكل أساسي وفي مجال جمع المعلومات، كما أنها استخدمت في المظاهرات الحشود والاجتماعات غير المرغوب فيها من الناحية الأمنية. كما أنه قد تم استغلال التقنيات الشائعة الاستخدام كالهاتف لهذه الغاية، فتم رصد المحادثات الهاتفية والتنصت وتسجيل المكالمات عن بعد، واعتراض المكالمات الهاتفية، والفاكس والجوال.

كما استخدم الكثير من المعدات المساعدة في المعلومات كالحبر وما يسمى الحبر السري والحبر الكيميائي المشع، وتطور استخدام هذه التقنيات بشكل أكثر خطورة فقد طورت أدوات قتل على شكل أقلام حبر، وأدوات عادية (كاميرا) ووضع أدوات التنصت في كل مكان على شكل صورة طفل أو في إطار خشبي أو في الاضاءة، أو

في سور المنزل، أو في منفضة السجائر، أو على شكل ربطة عنق، أو قميص، أو هدية، أو ساعة يد . . . إلخ.

وفي إسرائيل مدرج تتجمع فيه الأسر الإسرائيلية في يوم المخابرات وفيه متحف بالمقتنيات والأدوات التي استخدمت في المخابرات ومنها جهاز إرسال في قاعدة مكواة، وميكرفون في غلاية للقهوة وحبر خفي في زجاجة عطر، وجهاز تسجيل سجل المحادثة السرية بين الملك حسين والرئيس جمال عبد الناصر والتي كانت نذيراً بحرب الأيام الستة، وفيها الزي التنكري الذي ارتداه يعقبوئية عندما تسلل للأردن، وخرج منها حتى اعتقل فيها وأعدم عام 1949، وجهاز اللاسلكي البلوري الذي استخدمه بنت وموشيه مرزوق في إدارة الموساد في مصر حيث ماتا في السجون المصرية (توماس، 1999، موثق في الخليفة، 2000).

وإسرائيل بارعة في نسخ ونقل التكنولوجيا، فما إن تصلها أي تكنولوجيا جديدة حتى تنسخها وتقلدها. وتقدمت إسرائيل كثيراً في مجال الإنترنت ولديها الخبرة والتقانية معاً.

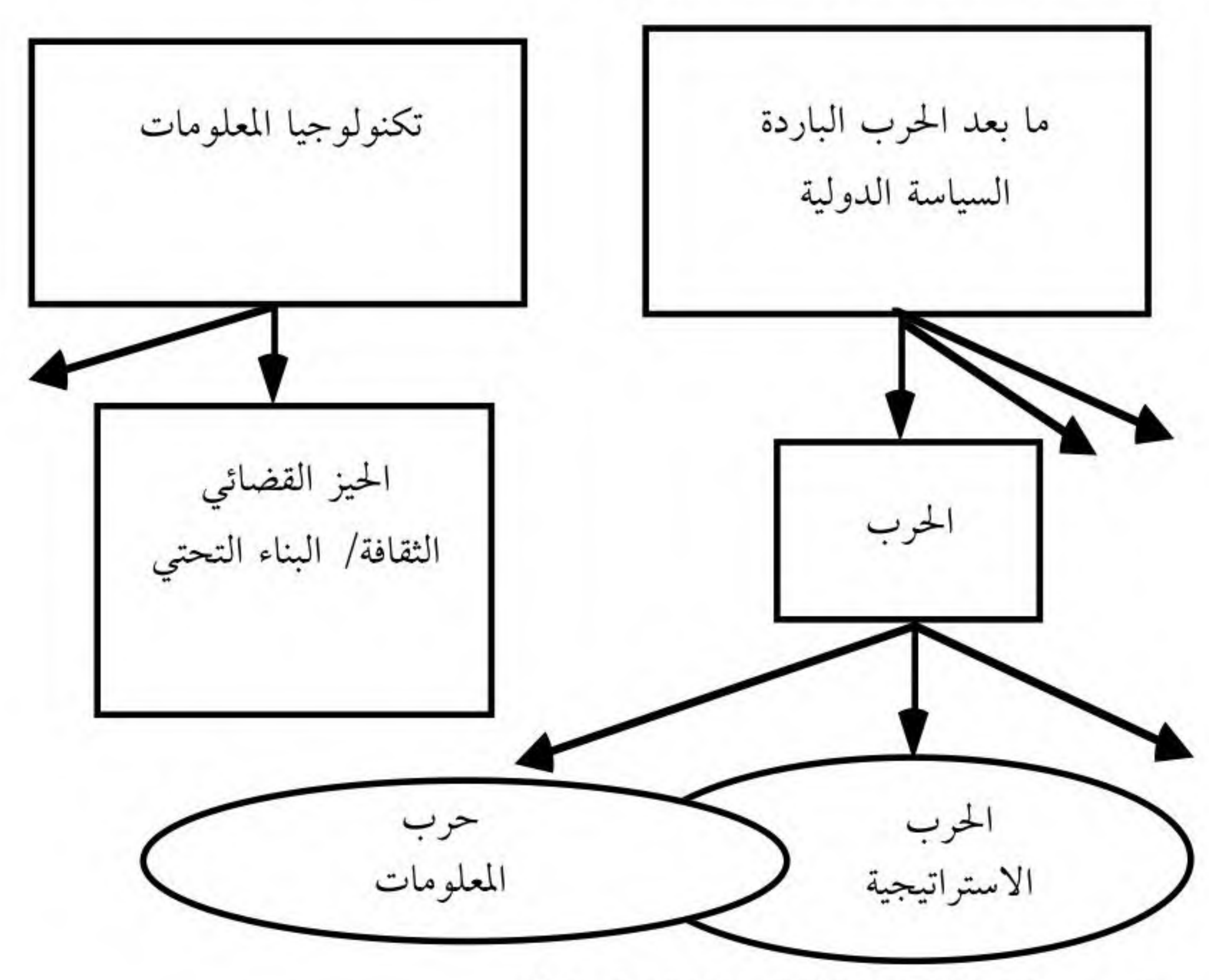
ولم تعد أدوات التجسس بحكر على أجهزة الاستخبارات والمخابرات، فيمكنك زيارة موقع متجر التجسس على الإنترنت (Spy Shop) وحيث النماذج الحديثة والرخيصة الثمن وعلى أشكال ونماذج متعددة، ويشمل المتجر على آلات التصوير على شكل ربطة عنق أو كاميرات صغيرة، أو ميكروفونات، أو العاب . . . إلخ. (htt://www.spysupply007.com).

حرب المعلومات الاستراتيجية Strategic Informational Warfare

بدأ مفهوم حرب المعلومات الاستراتيجية في الظهور في حرب المعلومات، ويعني استخدام الدول الحيز الفضائي للتأثير على العمليات العسكرية الاستراتيجية لايقاع التخريب في البنى التحتية الوطنية. إن حرب المعلومات وما بعد الحرب الباردة فد أدتا إلى ادراك خاص وانتباه للوجه الجديد للحرب مع تطبيقات في الاستراتيجية العسكريةوالاستراتيجية الخاصة بالامن الوطني.

لقد ظهور البناء التحتي للحيز الفضائي والثقافة خارج السياق العسكري (مع العلم بمساهمة وزارة الدفاع في ظهور الانترنت). ان ظهور خصائص وعناصر الحيز الفضائى

قد وفرت فرصاً لحرب المعلومات. وهناك تطور مستمر للسياسة الدولية ومع هذا السياق تطورت حرب المعلومات الاستراتيجية كأداة سياسية. ان تطور في حرب المعلومات الاستراتيجية يشمل بعداً في تهديدات الحيز الفضائي والانكشافات وهذان يمكن تسميتهما حرب المعلومات الاستراتيجية.



المصدر: Molander, Riddile & Wilson, 1996, p.2

شكل رقم (4)

العمليات الهجومية والدفاعية في حرب المعلومات الاستراتيجية

شكل وزير الدفاع الامريكي المجلس التنفيذي لحرب المعلومات (IW Executive Board) لتسهيل وتحقيق اهداف حرب المعلومات. طُلب من (RAND) تقديم تمرين لتحليل الاطار العام لتحديد المواضيع الرئيسة لحرب المعلومات واكتشاف نتائجها وابراز النقاط الرئيسة لوضع سياسية حرب ومعلومات، وللمساعدة في تطوير اجماع وطني دائم الاستراتيجية العامة لحرب المعلومات.

ولقد قامت RAND بتكوين اطار مبنى على التمرين والتحليل بتمرين عرف باسم "حرب المعلومات الاستراتيجية" شمل اعضاء من الامن الوطني ومن الاتصالات ذات الصلة، وصناعات نظم المعلومات ويقوم التمرين على ازمة حرب معلومات تشمل مناطق رئيسية، وقد سمي هذا التمرين اليوم الاخر (The Day after) والسيناريو المستخدم لهذا التمرين هو اسدال الستار على صراع القرن بين ايران والولايات المتحدة وحلفائها مركزين على تهديد للسعودية من قبل ايران. لقد طبق التمرين (6) مرات في صيغ مختلفة على مدار (5) أشهر في الفترة (1-1990/6) لقد بدأ التمرين منطلقاً من الجانب الاساسي في حرب المعلومات الاستراتيجية وهو عدم وجود " خط مواجهة " وأن الاهداف الاستراتيجية في الولايات المتحدة عرضه للهجوم كما هو في المسرح، والتحكم، والاتصالات (C3I). لقد حدد للتمرين اربعة مسارح منفصلة ومتميزه وهي (1) ميدان المعركة، و (2) الحلفاء، (المنطقة الداخلية، وهي السعودية). (3) منطقة القارة للاتصالات والحشود (الخليج العربي) (4) المنطقة الداخلية للولايات المتحدة وحرب المعلومات (المفترض وقوعها) على هذه المناطق الاربعة .

ان خلاصة التمرين قد انبثقت عنها خمسة توصيات هامة هي:

1- **القياة** (Leadrship) **من هو المسؤول في الحكومة؟**

ان الخطوة الاولى والهامة هي تقدير النقطة المركزية لقيادة الحكومة في دعم الاستجابات لمسرح حرب المعلومات الاستراتيجية، وهذه النقطة المركزية يجب أن تكون في المكتب التنفيذي الرئيس وهذا المكتب مسؤول عن التنسيق مع الجهات ذات العلاقة والقطاعات الحكومية الاخرى. ان تأسيس مستوى قيادة عليا يجب أن يأخذ المسؤولية لتنفيذ وادارة مراجعة شاملة لمواضيع حرب المعلومات الاستراتيجية الوطنية.

2- **تقدير الخطورة (** Risk Assessment)

ان مهمة القيادة الحكومية المشار اليها اعلاه وكخطوة أولى هي تنفيذ تقدير للخطورة فوري وذلك لتحديد إلى درجة مدى الثغرات في العناصر الرئيسية في الامن الوطني والاستراتجية العسكرية الوطنية وحرب المعلومات الاستراتيجية، ويجب ان تشمل المراجعة قواعد الاهداف الاستراتيجية، وآثار حرب المعلومات، والثغرات

الموازية وتقديرها وبدون تقدير الخطورة فإنه يصعب على القيادة العليا (الرئيسي) اتخاذ اساس لاتخاذ قراات في مواضيع حرب المعلومات الاستراتيجية، خاصة مع وجود نسبة متفاعلة من التغيرات في كل من تهديدات الحيز الفضائي والثغرات .

3- **دور الحكومة** (Governments Role)

لقد ظهر من التمرين الحاجة إلى مناقشة دور مناسب للحكومة في مهددات حرب المعلومات الاستراتيجية وفي ادراك هذا الدور (جزء من القيادة وجزء من المشاركة في القطاع المحلي) سوف يتطور مثل هذا الدور. من مثل التنظيم والتدريب وادامه القوى العسكرية - فإن الحكومة يمكن ان تلعب دوراً منتجاً وفاعل كمسهل ومُديم لبعض النظم المعلومات والبنى التحتية المعلوماتية ومن خلال الميكانزمات السياسية مثل (وقف الضرائب) لتشجيع خفض الثغرات وتحسين قدات اعادة المؤسسة والاستعادة ويجب الموازنة بين دور الحكومة في مثل هذا المجال وادراك العامة بفقدان الحريات المدنية واهتمام القطاع التجاري حول الحدود غير المضمونة لممارساته واسواقه.

4- **استراتيجية الامن الوطني** (National Securiety Strategy)

عندما يتم استكمال تقدير الخطورة فإن استراتيجية الامن الوطني تحتاج الى مناقشة الاستعدادات للتهديدات المحددة وهذه الاستعدادات تتقاطع مع عدد من الحدود التقليدية من "الجيش" الى "المدني" ومن " الوطني" الى " المحلي " ان احد وسائل مئسسة مثل هذا النوع من الاستعدادات ما سمي البناء التحتي المعلوماتي الاساسي الادنى (MEII) والذي قدم كمشوع ممكن في حرب المعلومات الاستراتيجية الدفاعية في التمرين والبناء التحتي المعلوماتي الاساسي الادنى يشمل ادنى مزيج (Minimum) من نظم المعلومات، والاجراءات، والقوانين، والمعززات الضريبية. إن احد النقاط الرئيسة للبناء التحتي المعلوماتي الأساسي الادنى هي تحديد القواعد، والتنظيمات المدعومة من الحكومة لتشجيع المالكين والمشغلين للبنى التحتية المختلفة لاخذ الاجراءات لحفض انكشافات بناهم التحتية وتأمين اعادة مئسستها في وجة تعديات حرب المعلومات الاستراتيجية والمفهوم المرادف لذلك في الاستراتيجية الذرية هو "شبكة اتصالات الطوارىء الاساسية الدنيا" (Minimum Essential Emegecy Commuications Network (MEECN)) حيث وجد ان هذه البنية مناسبة في مفاهيمها لحرب المعلومات الاستراتيجية.

خصائص حرب المعلومات الاستراتيجية:

1- **مدخلات قليلة الكلفة**: تمتاز حرب المعلومات الاستراتيجية بانها لا تتطلب كلفة مادية كبيرة أو دعم حكومي كبير كما هو الحال في الحرب التقليدية، المتطلب السابق لحرب المعلومات الاستراتيجية هو خبراء نظم المعلومات وإمكانية الدخول الى الشبكات المهمة. ان الشبكات المترابطة عرضة للهجوم والتخريب ليس فقط من قبل الدول ولكن من جهات غير الدول بما في ذلك الجماعات والافراد.

2- **حدود تقليدية غير واضحة**: لقد تعقد التمييز التقليدي- بين كل من الاهتمامات العامة-الخاصة، والسلوك المستقيم- المجرم الحدود الجغرافية (مثل التي بين الدول) - مع التطور في التفاعل داخل البنى التحتية المعلوماتية.

3- **الدور المتنامي لادارة الادراك**: ان تقنيات المعلومات الجديدة ربما تزيد بشكل ملحوظ نشاطات التأثير، و قوة الخداع وانتقاء الصور (Image-manipulation) كما يؤدي إلى تعقيد جهود الحكومة في بناء دعم سياسي للمشاريع الامنية ذات العلاقة .

4- **تحد استخبارات استراتيجي جديد**: ان الفهم الضعيف للثغرات في حرب المعلومات الاستراتيجية والاهداف يؤدي الى ازالة فاعلية طرق جمع الاستخبارات التقليدية وتحليلها . ولقد تطور حقل جديد في حرب المعلومات الاستراتيجية.

5- **مشكلات التحذير التكتيكي المرعب وتقدير التعدي**:لا يوجد حالياً نظام تحذير تكتيكي مناسب للتميز بين هجمات حرب المعلومات الاستراتيجية والهجمات الاخرى لنشاط الحيز الفضائي بما في ذلك التجسس او الحوادث .

6- **صعوبة بناء تحالفات دائمة والمحافظة عليها**: ان الاعتماد على تحالفات يمكن أن يزيد الثغرات الامنية لجميع الشركاء الى هجمات حرب المعلومات الاستراتيجية .

7- **انكشافات الاراضي**: ان وسائل المعلومات قد لاشت الحدود الجغرافية. ان الاراضي منكشفة للتعديات مثلها مثل الاهداف في المسرح وخاصة مع زيادة الاعتماد على البنى التحتية المعلوماتية.

الفصل الخامس

حرب المعلومات : النظرية

مقدمة

تأخذ حرب المعلومات اشكالاً متنوعة، فمنها السياسي الذي يهدف الى التأثير على عقول القادة ومتخذي القرار، ومنها العسكري الذي يهدف الى تدمير المعلومات ونظمها العسكرية واستغلالها أو الحرمان من استخدامها أو توظيفها ضد العدو، ومنها التجاري الذي يهدف الى سرقة الاسرار التجارية للشركات وخاصة المنافسة واستثمارها أو تدمير سمعتها، ومنها الشخصي الذي يهدف الى اغتيال السمعة الشخصية للافراد والجماعات.

ولم تعد حرب المعلومات حرباً بين الدول، بل اصبحت حرباً من الدولة ضد رعاياها، فجمع المعلومات من خلال المظاهرات ومراجعة اشرطة البث الفضائي وتحديد هوية الاشخاص المشاركين واستجوابهم واعتقالهم قد اصبح من الاساليب المألوفة في الدول النامية، أما الدول المتقدمة فتستخدم اساليب اخرى لخرق خصوصية شعوبها، فمنها ما اقرته الولايات المتحدة بعد هجمات 2001/9/11 والمعروف بقانون باتريوت (PATRIOT) والذي يعني توفير الوسائل اللازمة لاغراض الارهاب وصده. وهذا يعني ان الدوائر الامنية ستتمكن من التنصت والتجسس على المواطنين بحجة صد الارهاب واعتراضه، وتسجيل مكالماتهم وخرق خصوصياتهم. ولقد مكن هذا القانون من استخدام برمجيات تنصت وتجسس على الآخرين وخاصة ما عرف باسم المفترس (Carnivore) وهذا البرنامج الذي أثار ضجة، ذلك انه يُمكن الاجهزة الامنية من تسجيل البريد الالكتروني الوارد والصادر للشخص المعني والتجسس على المواقع الالكترونية.

مفهوم حرب المعلومات

يعد مفهوم حرب المعلومات (Information Warfare) من المفاهيم الغامضة، ولكن المستخدمة بكثرة لوصف حرب المستقبل، أو الحرب المرتبطة بعصر المعلومات. إن جذور حرب المعلومات قديمة، ومن أهم المبادئ القديمة في حرب المعلومات المفاجئة (Surprise) والسرية. ولقد وصف صن تزو (Sun Tzu) عملية استغلال المعلومات في الحرب بقوله:

«إن معرفتك لعدوك ومعرفتك لنفسك في مئات المعارك لن تجعلك تخسر أو تتعرض للخسارة. وعندما تتجاهل عدوك وتعرف نفسك فإن فرصتك في النصر أو الهزيمة متساوية. أما إذا تجاهلت نفسك وعدوك، فتأكد أنك ستكون الخاسر في كل معركة»(Tzu/Griffith, 1963, p. 84)

إن هدف حرب المعلومات في أيام الحرب هو عقل الإنسان وخاصة العقول التي تتخذ القرارات وخاصة العسكرية أو المعروفة بالعمليات النفسية (Psyop). وحرب المعلومات صراعات تتضمن حماية المعلومات (Protection)، وانتقاء المعلومات (Manipulation)، وتخريب المعلومات (Degradation)، والحرمان من استخدام المعلومات (DOS). وهذه تشمل السيطرة والتحكم (C2)، والاستخبارات والحرب الإلكترونية (راديو، تشفير) والحرب النفسية، وحرب الدخلاء، وحرب الاقتصاد المعلوماتي، والحرب الفضائية (Stein, 1996)

إن أبسط تعريف لحرب المعلومات هو استخدام المعلومات في تحقيق الأهداف (المصالح) الوطنية. فالمعلومات مفتاح للقوة الدولية، وهي مصدر وطني حيوي يدعم الدبلوماسية والاقتصاد . . . إلخ. وتأثير المعلومات هام خاصة في مجالات الأفكار والمعاني، والتفكير الإنساني، والطريقة التي يتخذ بها القرار، والتأثير على الإنسان وعلى القرارات التي يتخذها، وقد تستخدم لتكوين سوء مزاوجة بين الخصوم.

تعني حرب المعلومات (Information Warfare) تخريب المعلومات أو تدميرها أو سرقتها أو تحريفها، أو أساءة استخدامها، أو المنع من الوصل إليها، أو تقليل موثوقيتها، أو استخدامها ضد أصحابها. إنها باختصار استخدام المعلومات ضد المعلومات، إنها سرقة الاسرار، إنها قلب المعلومات ضد أصحابها، إنها حرمان الطرف الآخر (العدو) من استخدام معلوماته أو منعه من استخدام تقنياته ومعلوماته إنها تحول الطرف المستهدف إلى أصم وأبكم، وأعمى معلوماتياً مما يسهل التحكم به والسيطرة عليه.

حرب المعلومات هي حرب عصر المعلومات، وربما حرب ما بعد عصر المعلومات. والحرب عادة ما تتطور بتطور المجتمعات شأنها في ذلك شأن الكثير من السلوكيات والأفعال في المجتمع. فالحرب في المجتمع الزراعي تختلف في أساليبها وأهدافها عنها في المجتمع الصناعي وعنها في عصر المعلومات أو في المجتمع المعلوماتي.

حرب المعلومات مبنية على قيمة مصادر المعلومات لكل من المهاجم والمدافع. فعملية الهجوم تهدف إلى زيادة القيمة للهدف في حالة الهجوم، بينما تقلل قيمته في حالة الدفاع. وتحاول عملية الدفاع مواجهة احتمال الخسارة في القيمة. كما أن حرب المعلومات هي عملية "كسب ـ خسارة". وأنها تتعلق بالحرب بالمفهوم العام الشامل لها مواجهة أنواعاً محددة من الجرائم والعمليات العسكرية.

وتعني حرب المعلومات استخدام المعلومات ونظمها في العدوان والدفاع المعلوماتي، وذلك لاستغلال المعلومات ونظمها، أو تخريبها أو تدميرها لدى الخصم، والمحافظة على المعلومات ونظمهاسليمة. وتهدف هذه الأفعال إلى تحقيق تقدم على جيش العدو وأعماله الأخرى الداعمة للمجهود الحربي. وتمثل حرب المعلومات صراعاً على امتلاك المعلومات والسيطرة عليها، وهذا الصراع يحدث على مستويات ثلاثة هى :

أ. الصراع الفكري للخصم (Ideational Struggle) ويشمل الآليات النفسية والإعلامية والدبلوماسية والعسكرية المؤثرة في عقل الخصم سواء كان الخصم قائداً عسكرياً أو مجتمعاً بأكمله.

ب. السيطرة المعلوماتية (Information Dominance)، ويشمل هذا المستوى السيطرة على شؤون الصراع المادي.

ج. الدفاع عن التدفق المعلوماتي، ويشمل التصدي للهجوم على أي بناء معلوماتي عسكري أو مدني بما في ذلك مواجهة الدخلاء والمتطلفين والتدمير المادي للأبنية المعلوماتية والخداع والعمليات النفسية.

لقد جمَّع المركز الاستراتيجي للدراسات الدولية (CSIS) الأدبيات الخاصة بحرب المعلومات بناءً على المصدر والنوع والأهداف، ونظر إلى حرب المعلومات كمزيج من هذه الأبعاد. والخلاصة هي أن حرب المعلومات الهجومية يمكن أن تكون من الداخل، أو الخارج وأن أشكال العدوان المعلوماتي تتراوح بين الهجوم على البيانات والبرمجيات والدخول غير الشرعي والقرصنة والهجمات المادية على مواقع المعلومات. أما الأهداف فيرى المركز أن هناك أربعة أهداف رئيسة لحرب المعلومات هي :

1-الاستغلال، و2- الخداع، و3- خلق الفوضى، وأخيراً 4- التدمير للمعلومات ونظمها (Ehlers, 1999).

ويعرفها (USAF) على أنها «أي فعل داخل بيئة المعلومات الهدف منه حرمان، أو استغلال أو تخريب، أو تدمير معلومات الخصم، نظمه المعلوماتية وعملياته المعلوماتية في الوقت الذي تحمي فيه القوات الصديقة من هذه الأفعال» (USAF, 1995, p. 20). وهذا يعني تدمير محطات الإرسال والهاتف والتلفزيون والحاسبات كل هذا يقع ضمن حرب المعلومات.

ويرى توفلر وآخرون أن مفهوم حرب المعلومات يشمل العمليات ذات الأساس المعلوماتي التي تؤثر على «العواطف والدوافع، والتبرير المنطقي، وسلوك الآخرين» (Stein, 1996).

وتعرف وكالة نظم الدفاع المعلوماتية الأمريكية (DISA) حرب المعلومات بأنها «الأفعال المنفذة لتحقيق تفوق معلوماتي لدعم الاستراتيجية العسكرية الوطنية من خلال التأثير في معلومات الدعاية ونظم المعلومات . . . في الوقت الذي تحمي وتصان المعلومات ونظمها لدينا»، ويشمل هذا التعريف ثلاث فئات رئيسة في حرب المعلومات هي:

1- العدوان (Offensive)

و2- الدفاع (Defensive)

و3- الاستغلال (Exploitation).

ويمكن النظر إلى هذه الفئات من خلال الأعمال العدوانية المعلوماتية والتي تتضمن الحرمان من الخدمة، والإفساد المعلوماتي، والتدمير المعلوماتي، والاستغلال المعلوماتي، أو التأثير على إدراك الخصم، وحماية البنية التحتية المعلوماتية من الاعتداءات المشار إليها أعلاه، واستغلال المعلومات المتاحة وفق الزمن لتسريع القرار أو دائرة الفعل وافساد دائرة الخصم.

كما تعرف وزارة الدفاع الأمريكية (DOD) حرب المعلومات على أنها «الأفعال المتخذة لتحقيق التفوق المعلوماتي من خلال التأثير في معلومات الخصم وعملياته ذات الصلة بالمعلومات ونظمها والشبكات ذات الأساس الحاسوبي، في الوقت الذي تتم فيه حماية المعلومات والعمليات ذات الصلة بالمعلومات ونظمها والشبكات ذات الأساس الحاسوبي الخاصة بنا» (Girard, 1998, p. 2).

يعرف ون شوارتاو حرب المعلومات على أنها «صراع إلكتروني حيث تكون المعلومات حيزاً استراتيجياً يستحق السيطرة أو التدمير» (Schwartau, 1994, p. 13).

ويعرفها ايمتبياج مساعد سكرتير الدفاع لشؤون القيادة والسيطرة والاتصالات والاستخبارات (Assistant Secretary of Defense, Command, Control, Communicution and Intelligence [ASD/C3I]. بأنها «الأفعال المنفذة بقصد تحقيق سيطرة معلوماتية من خلال التأثير على العمليات ذات الصلة بالمعلومات لدى الخصم، ونظم المعلومات، وشبكات الحاسب، وحماية معلوماتنا، والعمليات ذات الصلة بالمعلومات ونظم المعلومات وشبكات الحاسب التي تخصنا» (موثق في Fredericks, 1996, p. 3). ويشمل هذا التعريف بأن حرب المعلومات تشتمل على إجراءات دفاعية وهجومية، أما الإجراءات الهجومية فهي تلك الأفعال المتخذة ضد معلومات الخصم ونظم معلوماته، بينما تتركز الإجراءات الدفاعية بالأفعال المتخذة لحماية معلوماتنا ونظمها والبنية التحتية المعلوماتية الوطنية. والإستراتيجية الناجحة تشمل الاثنين.

ولقد توصلت جامعة الدفاع الوطني الأمريكية إلى التعريف التالي لحرب المعلومات: «اتجاه في الصراع المسلح يركز على إدارة واستخدام المعلومات بكافة أشكالها وعلى جميع المستويات لتحقيق ميزات عسكرية في البيئات المشتركة والمدمجة. حرب المعلومات هجومية ودفاعية في طبيعتها، وتتراوح بين الإجراءات التي تحول دون استخدام العدو لاستغلال المعلومات إلى الإجراءات المقابلة لتأكيد وحدة وتوافر، وتفسير رأس المال المعلوماتي، وتشن حرب المعلومات في مجالات السياسة والاقتصاد والاجتماع، وتنطبق على كامل الأمن الوطني من السلام إلى الحرب. كما تركز حرب المعلومات على حاجات السيطرة والتحكم من خلال تطبيق التقنيات المعلوماتية للسيطرة والتحكم من خلال تطبيق التقنيات المعلوماتية للسيطرة على المعارك الأرضية» (IRMC of the NDU, 1993).

هناك جانبان لحرب المعلومات حيث تعمل كل من العمليات الهجومية والدفاعية من خلالهما وهما :

1- الانتقاء غير المباشر للمعلومات، حيث يتم التأثير في معلومات العدو من خلال عمليات الإدراك والتحليل، وقد يكون هذا من خلال عدم تمكين العدو القدرة على الملاحظة من خلال التشويش (Jammers)، أو تدمير الرادارات

. . . إلخ. وبالمقابل يمكن تغذية العدو بمعلومات خاطئة مما يجعله يعتقد بشيء خطأ أو أن لا يعتقد بشيء صحيح، أي يقبل الخطأ ويرفض الصحيح، وهنا تستخدم التقنيات الحديثة وخاصة الفضائية وكذلك العمليات النفسية من خلال الرسائل الموجة بالمنشورات أو الراديو أو التلفزيون أو الإنترنت . . . إلخ. والهادفة إلى إدارة إدراك الخصم لصالح الطرف المهاجم.

2- الانتقاء المباشر للمعلومات الخاصة بالخصم من خلال تمرير رؤيته، وتحليله أوعمليات قراراته. وما تعنيه حرب المعلومات هنا هو استخدام المعلومات كبديل عن الطرق التقليدية في القتال وليس أداة موازية لها. ومن أساليب حرب المعلومات المباشرة فيروسات الحاسب، والقنابل المنطقية، تعديات الدخلاء، على سبيل المثال فقد أفادت (US News) و(World Report) أن المخابرات الأمريكية نجحت في إصابة شبكات الحاسب الخاصة بالدفاع الجوي العراقي بفيروس مما سبب اختفاء المعلومات (US News & World Report, 1992).

أما وزارة الدفاع الفرنسية (FMD) فترى أن حرب المعلومات تشمل ثلاثة أركان أساسية هي (1) الحرب من أجل المعلومات (War for Inforamtion)، وهي حرب تهدف إلى الحصول على المعلومات عن أهداف العدو وقدراته واستراتيجياته لنتمكن (نحن) من الدفاع عن أنفسنا، (2) الحرب ضد المعلومات (War Against Information)، وتتعلق بحماية (الدفاع) المعلومات ونظمها لدينا وتدمير (الهجوم) معلومات ونظم العدو، (3) الحرب من خلال المعلومات (War Through Infromation) وهو استخدام المعلومات كمصدر هام وحيوي للسيطرة على المعلومات الخاصة بالعدو وتحسين الحصانة المعلوماتية والدفاعات المعلوماتية لدينا (Ehlers, 1999).

أما جالدي (Galdi) فعرف حرب المعلومات بأنها: (1) مهاجمة، أو التأثير، أو حماية القوة العسكرية، والمراقبة والاتصالات، والسيطرة والتحكم، والدفاع المدني والثروة الاستخبارية. (2) مهاجمة أو التأثير على أو التعدي على روابط الاتصالات الأساسية في المجتمع ـ نقل الصوت، والصورة أو البيانات والطاقة الكهربائية أو نظم التحكم والهاتف. (3) استخدام التلفزيون والراديو أو المواد المطبوعة للمهاجمة أو التأثير أو لحماية اتجاهات الجنود والمجتمع المعني أو القادة (Galdi, 1995, p. 7).

أما راثمل (Rathmell) فيعرفها على أنها «الصراع من أجل السيطرة على نشاطات المعلومات»، ولقد ميز ثلاثة مستويات من حرب المعلومات هي :

1- المستوى الأعلى (Highest Level)، وهو صراع الأفكار لعقل الخصم وهذا يشمل مدىً واسعاً من العمليات النفسية والإعلام والأساليب الدبلوماسية والعسكرية للتأثير على عقل الخصم سواء كان عسكرياً أو قائداً أو على السكان عامة.

2- المستوى الثاني وهو يماثل مضامين إدارة الخطورة (RMA) والتي تهدف إلى السيطرة على المعلومات.

3- المستوى الأدنى ويشمل التصدي لتدفق المعلومات ونشاطاتها ويتراوح بين الهجمات الإلكترونية مثل القرصنة، والتدمير المادي، والتضليل والعمليات النفسية (Rathmell, 1998, p. 6).

وهناك ثلاث مجموعات فرعية يمكن أن تستخدم حرب المعلومات هي:

1- جمع المعلومات الاستخباراتية، والاتصالات، وغسيل الأموال، والدعاية (الحرب النفسية).

2- التعدي المادي على النشاطات المعلوماتية لمستهدف معين.

3- استخدام أساليب التعدي الرقمي ضد النشاطات المعلوماتية لمستهدف معين (Aquilla & Ronfeldt, 1993).

لقد صنف شوارتو (Schwartu) حرب المعلومات إلى ثلاثة مستويات هي: حرب المعلومات الشخصية، والمؤسسية،والكونية، ويمكن إضافة مستوى رابع يحتل الترتيب الثالث وهو المستوى الوطني.

1ـ **المستوى الأول** : حرب المعلومات الشخصية (Personal Information Warfear)، ويشمل هذا المستوى التعديات علي خصوصية الأفراد الإلكترونية وهذا يشمل كشف السجلات الرقمية وقواعد المعلومات التي خزنت فيها المعلومات الشخصية. وفي عصر المعلومات فإن سيطرة الإنسان على المعلومات الخاصة به ضعيفة خاصة وأن هناك الكثير من المعلومات والسجلات الحكومية والخاصة (السكان، والصحة، والعمل . . . إلخ.) التي يمكن الوصول إليها بسهولة، ويقلق حوالي (70٪) من الأمريكان على فقدانهم خصوصيتهم (Schwartau, 1994). ويمكن النظر إلى هذا المستوى على أنه حرب وتعدٍ على المجال الفضائي الفردي (Individual Cyberfield).

2ـ **المستوى الثاني** : حرب المعلومات المؤسسية (Corporate Information Warfare)، ويمثل هذا المستوى التنافسي بين المؤسسات المحلية والعابرة للحدود الوطنية (الكونية)، فمن الممكن أن تتمكن شركة من سرقة تصاميم وبرامج شركة أخرى أُنفق على تطويرها ملايين الدولارات. هذا بالإضافة إلى نسخ التكنولوجيا فالمعروف عن اليابان واسرائيل قدرتهما العالية على التقليد والنسخ للتقنيات التي يتم الحصول عليها بطريقة شرعية وتطويرها بأشكال متقدمة ومختلفة، ومن الأمثلة على ذلك طائرات التجسس التي باعتها إسرائيل للصين واعترضت على ذلك الولايات المتحدة الأمريكية لأنها طائرات أمريكية ولكن الإسرائيليين قد عدلوا عليها، وهذا النوع من التجسس هام ونشط في المجال العسكري والاقتصادي وخاصة بين الروس والأمريكان وبين الصين وأمريكا.

3ـ **المستوى الثالث** : حرب المعلومات الوطنية (National Information Warfare). ويشمل هذا المستوى حرب المعلومات التي يستهدف البناء التحتي المعلوماتي الوطني، حيث يمكن أن تستخدم القنابل الكهرومغناطيسية أو فيروسات الحاسب أو أية أداة من أدوات حرب المعلومات في تدمير أو تخريب أو الحرمان من الخدمات لمكونات البناء التحتي المعلومات الوطني، فمثلاً يمكن تعطيل محطات الطاقة أو النظام المالي، والبنوك أو نظام الاتصالات أو المواصلات أو الملاحة الجوية، مما يؤدي إلى ارباك كبير وخسارة كبيرة جداً في هذه القطاعات وشل الحركة العامة لدى الناس ولدى المجتمع كله.

4ـ **المستوى الرابع** (الثالث عند شوارتو): حرب المعلومات الكونية (Global Information Warfare)، وهذا النوع موجه نحو الصناعات والقوى الاقتصادية الدولية، وقد يكون ضد مجموعة دول أو بلدان، أو ضد البناء التحتي المعلومات الكوني. ويمكن لشخص ما أن ينفق (200) مليون دولار في أسلحة الموجة الثالثة ويمكن أن يكون قادراً في (3) سنوات من تدمير الصناعة الأمريكية ويمكن أن يُحدث انهياراً في وول سترتيت (Wall Street) واغلاق نظام البنوك في الولايات المتحدة الأمريكية، وهذا يؤثر على شركات كثيرة عابرة للحدود الوطنية.

لقد استخدم الفن وهيدي توفلر أنموذجاً في وصف تاريخ الحروب مبيناً على ثلاث موجات هي:

1- **موجة الزراعة** (Agrarian Wave). لقد بدأت الثورة الزراعية أول درجة كبيرة من التغير في التاريخ البشري، ولقد أدت إلى تطور المجتمعات الحديثة، لقد

مكنت الزراعة المجتمعات من الإنتاج الاقتصادي والذي تسبب في العديد من الحروب. ولكن كان الرابط بين الحرب والأرض كبيراً في ذلك الوقت. ولقد كان العسكر مشغولين غالبية الوقت في العمل في الحقول. ولقد كان الجيش سيئ التنظيم والإعداد (باستثناء بعض الحالات مثل روما) وكانت رواتب الجيش ليست بالمال وإنما بأشياء مثل الأرض، وولاء الجيش عادة ما يكون لصاحب الأرض، ويعمل الجيش فترة طويلة في الزراعة وشهراً أو شهرين في الجيش.

2- **الموجة الصناعية** (Industrail Wave)، لقد غيرت الثورة الصناعية طريقة الحرب، إن عناصر الإنتاج الشامل أدت إلى إنتاج سلاح الدمار الشامل (الذري والكيماوي). ولقد كان ولاء العسكر للدولة وليس لصاحب الأرض. ولم يتم الانتقال من موجة إلى أخرى في فترة قصيرة، وخلال فترة الانتقال، مرت عدد من الحروب وقد تم خوضها وقد شملت كلا النوعين (الزراعي والصناعي)، ومن الأمثلة على ذلك الحرب الأهلية الأمريكية (1862-1863م)، حيث هزم الشمال الصناعي الجنوب الزراعي. ولقد كان التغير الرئيسي في انتاج الجيوش القياسية (المعيارية) ولقد استجابت الصناعة لاحتياجات ميدان المعارك، ولم تكن المعيارية لانتاج الأسلحة فقط، ولكن طبقت في تدريب الجيش، كما تغيرت الأوامر من لفظية شفوية (Oral) إلى كتابية (Written) مثل الملاحظات والمذكرات التي تستخدم في الأعمال التجارية. ولقد أصبحت مكننة الحرب من الخطوات الرئيسة في هذه الموجة. والحرب العالمية الثانية مثال لاستخدام أسلحة الدمار الشامل فتوفى (15) مليون عسكري، واستخدم الدمار الشامل حتى قبل تفجير هيروشيما الذري. ولقد طورت القنابل الاستراتيجية ، والصواريخ ذاتية الدفع كأدوات دمار شامل، وتم اضافة عناصر ذرية ومكونات كيماوية إلى الأسلحة.

3- **موجة المعلومات** (Information Wave)، مع نهاية السبعينات وبداية الثمانينات من القرن المنصرم بدأت موجة التكنولوجيا تغير مجتمعات الموجة الصناعية. ولقد بدأ تكوين مجتمع اتصالات، وترافق مع هذا التغير تغير في العقيدة العسكرية، ولقد ظهرت الثنائية بين هاتين الموجتين في حرب الخليج الثانية (1990-1991م). فقد استخدمت أسلحة الدمار الشامل كما في الحرب العالمية الثانية بقنابل كبيرة تدميرية ولكن تم استخدام أسلحة ذات تقنية عالية لتحديد الأهداف بدقة، وكان الخوف من أن يفشل الجيش المعتمد على التقانة العالية في البيئة الصحراوية ولقد استمرت هذه

المخاوف من أن خسائر الحلفاء ستكون كبيرة. وهذا كان من الممكن أن يحدث لوكانت الحرب حرباً بمستوى الموجة الثانية، لقد جهز الحلفاء المعركة بسلاح الموجة الثانية وخاصة (جو ـ أرض) وبقنابل من عام (1968) من مخلفات حرب فيتنام. وخلال هذا الوقت استخدمت طائرات الشبح الليلية (F-117A) بتدمير أهدافها في بغداد. ولقد استهدفت مراكز الدفاعات الجوية والاتصالات العسكرية لتعمية العراق. والجدول التالي يبين المقارنة بين الموجات الثلاث.

جدول رقم (13)

أنموذج الموجات الثلاث

واصف الموجة	الموجة 1(الزراعية)	الموجة 2(الصناعية)	الموجة3 (المعلومات)
الأمن المادي بواسطة	المقاتلون، المرتزقة والصناديد	المواطنون المهنيون	القادة ذوو المعرفةالمعلوماتية
القوى المسيطرة (الاجتماعية الاقتصادية والسياسية)	القبيلة، المدينة الدولة، الأسرة	الولاية ـ الأمة المصانع	تآلف الشركات
الاقتصاد مسيطر عليه من	التجارة	المال	الرموز
القدرة التدميرية القصوى	ملح البارود	WMD (ذري،كيميائي ... إلخ.)	مسح البيانات الحساسة
القيادة	هرمية	أوامر من أعلى لأسفل	أبنية سطحية، مستوى موظفين متدنٍ
حرب ذات أساس معلوماتي	نعم	نعم	نعم
تكنولوجيا المعلومات في الحرب	لا	نعم	نعم
حرب معلومات	لا	لا	نعم

المصدر: http://www.seas.gwu.edu/-reto/infowar/history.html

أما **جنسن** (Jensen) فقد لخص المراحل للحرب في كتابه حرب المعلومات: مبادئ حرب الموجة الثالثة، حيث يقول بتطور ثلاثة أنماط من الحرب وهي الزراعية والصناعية والمعلوماتية.

1- **الحرب الزراعية** (Agraian Warfare)، حيث اعتماد الإنسان على الطبيعة وعندما تعلم الإنسان الزراعة فلم يعد بحاجة إلى الصيد، والترحال ولقد تطورت المجتمعات وأصبحت إمكانية تخزين الغذاء ممكنة. (وأصبحت الحرب ممكنة بسبب ا لتنافس بين الدول على مصادر الغذاء)، اما الأسلحة فهي ما يحمل باليد، والمواد المتوافرة في البيئة الطبيعية. وأما الأهداف المرتبطة بهذه الفترة فكانت الحصول على فائض من الثروة وأصبحت الأرض دافعاً للحرب.

2- **الحرب الصناعية** (Industrial Warfare)، لقد تغيرت الحرب الطبيعية في القرن السابع عشر مع التوصل إلى القوة البخارية (Steam Power). وهذا التغير أدى إلى التسريع مع صناعة الأجزاء والمصانع، وتبع ذلك تطور حضري، ودخلت فكرة الجيش وأصبحت هذه الفترة تعرف بالحرب الصناعية والمرتبطة بعصر الصناعة، وجاءت معها الحرب الصناعية. وهنا تطورت آلات الحرب الرئيسة، وتنظيم الجيوش، والإنتاج الشامل، وأسلحة الدمار الشامل، وبدأت الصراعات (Jensen, 1997).

3- **حرب المعلومات** (Information Warfare)، إن الاعتمادية المتزايدة على المعلومات قد جعلت الحاجة ماسة إلى تغير الأنموذج التقليدي في الأمن والبحث عن أنموذج (Paradigm) جديد يأخذ بالحسبان مثل هذه الاعتمادية. لقد أصبحت البنية التحتية المعلوماتية والمعلومات أكثر عرضة للهجمات العدوانية، ويمكن لأي خصم أن يشن حرب معلومات على الطرف الآخر من أي مكان في العالم، وبالتالي فإن قدرة الدولة على إدراك الخطورة والدفاع عن المعلومات ضد أي هجوم معلوماتي عنصر حيوي لبقاء الدولة وحفظ الأمن الوطني (Gillam, 1997).

وتمثل حرب المعلومات استخدام المعلومات في تحقيق المصالح الوطنية، حيث تشكل المعلومات بحد ذاتها مفتاحاً للقوة الدولية، ومصدراً وطنياً حيوياً يدعم الدبلوماسية والاقتصاد، والسياسة والأمن. وهي تشمل الأفكار والمعاني والتفكير الإنساني، والطريقة التي يتخذ بها القرار والتأثير على الإنسان وعلى القرارات التي يتخذها. وقد تتخذ صور للتأثير على عقل الإنسان وخاصة العقول التي تتخذ القرارات وخاصة العسكرية من خلال العمليات النفسية (Psyop) والدعاية والتأثير على المعنويات.

نظرية حرب المعلومات

نظرية دورثي داينج في حـــرب المعلومـــات (Denning'sTheory of Information Warfare) تشتمل حرب المعلومات على عمليات هجومية ودفاعية ضد مصادر المعلومات والتي طبيعتها «كسب ـ خسارة». ويتم تنفيذ هذه الحرب لأن مصادر المعلومات لها قيمة لدى الناس. وتهدف العمليات الهجومية إلى زيادة قيمة الهجوم، وإنقاصه بالنسبة للدفاع. وتهدف العمليات الدفاعية إلى مقاومة احتمالات خسارة قيمة تلك المعلومات.

تقدم دورثي داينج (Denning, 2000 b, PP 22-76) في كتابها «الأمن وحرب المعلومات» نظريتها عن حرب المعلومات والتي تتكون من عناصر أربعة هي :

1- مصادر المعلومات (Inforamtion Resorces).

2- أطراف الصراع (اللاعبون) (Players).

3- عمليات الهجوم (Offensive Operations).

4- عمليات الدفاع (Defensive Operations).

وفيما يلي وصف مختصر للنظرية:

أولاً : مصادر المعلومات (Information Resources)

حرب المعلومات هي العمليات التي تستهدف أو تستغل مصادر المعلومات. ويمكن تصنيف مصادر المعلومات وفق وظائفها إلى خمس فئات وهي: الحاويات (Containers)، والناقلات (Transproters)، والحساسات (Sensors)، والمسجلات (Recorders)، والمعالجات (Processors). وهذه الفئات لا تنفصل عن بعضها انفصالاً تاماً، إذ أنه يمكن أن يقوم مصدر ما بوظائف متعددة في الوقت ذاته مثل الأفراد، وأجهزة الكمبيوتر.

1ـ **الحاويات** : وهي أوعية المعلومات، وهي التي تحدد نوع تركيبتها، وإن كل هدف بذاته هو حاوية معلومات، إلا أن أهم هذه الأهداف هو ما يمكن أن يُعطى محتوى إضافياً. وتتضمن هذه الحاويات كلاً من: الذاكرة البشرية، الذاكرة الآلية في أجهزة الكمبيوتر، والمطبوعات، والأشرطة، والأسطوانات والأقراص الصلبة

وحاويات كل منها. ويمكن "تعشيش" الحاويات وإدخالها ببعضها (كالصندوق الصيني). فعلى سبيل المثال، يمكن الاحتفاظ بوثيقة في ملف للوثائق، وتوضع في خزانة ملفات، والخزانة في مكتب، والمكتب في مبنى، وهكذا. وتحفظ المعلومات عادة على أجهزة الكمبيوتر في وثائق، وتحفظ الوثائق ضمن ملفات. ويجب أن يتم اجتياز كل طبقة من هذه الطبقات في العالم العضوي الذي يمثل الخطوط الدفاعية للوصول إلى المعلومات. وأما في عالم الإلكترونيات، فيمكن تجاوز الطبقات الدفاعية هذه والموجودة ضمن البرامج. فيمكن مثلاً قراءة المعلومات الموجودة على قرص حاسب ما مباشرة، دون فتح الملف أو قاعدة البيانات التي يتم حفظها فيها، ولا داعي للمرور في نظام الأدلة لفتح المعلومات.

2ـ **الناقلات** : وهي أجسام وأنظمة اتصالات تنقل البيانات من مكان إلى آخر. وتشتمل الناقلات على كل مما يلي: الأفراد الذين ينقلون المعلومات الموجودة لديهم، ويحملونها معهم أينما ذهبوا، أو يبلغونها وجهاً لوجه شخصياً، والعربات أو وسائل المواصلات الأخرى، بما في ذلك الشاحنات، والطائرات، وأنظمة البريد بمختلف أنواعها، وأنظمة الاتصالات المعروفة بالدوائر من نقطة إلى نقطة (PPP)، بما في ذلك أنظمة البريد والبرق، والإذاعة بما في ذلك المسموعة والمرئية، وشبكات الكمبيوتر بما في ذلك الإنترنت وشبكات الشركات المختلفة.

3- **الحساسات** : وهي أجهزة التحسس التي تستطيع استخراج معلومات من أهداف أخرى ومن البيئة بشكل عام. وتتضمن هذه أجهزة التحسس البشرية، وآلات التصوير بأنواعها، والميكروفونات، والماسحات الإلكترونية والرادارات.

4ـ **المسجلات** : وهي أجهزة تضع المعلومات في حاويات. وتتضمن هذه الأجهزة كلاً من العمليات البشرية، والطابعات، والمسجلات الصوتية، والرقمية والمسجلات على الأقراص المدمجة، وعلى أقراص ال (DVD).

5- **المعالجات**: وهي أجهزة تبلور المعلومات وتعالجها، وتتضمن هي الأخرى كلاً من: البشر، والمعالجات المصغرة، وقطع الكمبيوتر وبرامجه. وتعمل هذه المصادر معاً بحيث تنساب المعلومات من حاوية معلومات إلى أخرى عبر مختلف نظم نقل المعلومات. وتلتقط الحساسات أو أجهزة التحسس المعلومات الموجودة في البيئة الفعلية، ثم تحولها إلى معلومات إلكترونية يفهمها الحاسب، ويمكن طباعتها، وإذاعتها

في الإذاعة أو التلفزيون، وبثها عبر مختلف أجهزة الإعلام والاتصالات والإنترنت، ويمكن تغذيتها في أجهزة تتحكم بالعمليات في البيئة مثل أجهزة التدفئة والتبريد. وإن هذا الترابط وإمكانية الاتصال بين مصادر المعلومات يتيح إمكانية إجراء عمليات حرب المعلومات التي تؤثر على المصادر غير المصادر التي تضرب مباشرة. وقد كان باستطاعة المتسللين المخربين مثلاً تغيير وجهة المكالمات الهاتفية بالعبث بالسجلات المحفوظة في أجهزة الكمبيوتر الخاصة بشركات الاتصالات. كما استطاعوا تخريب خدمات الاتصالات في المطارات بتعطيل أجهزة الكمبيوتر الموجودة في شركات الاتصالات.

ويشير مصطلح "البنية التحتية للمعلومات" (Information Infastructure) إلى مصادر المعلومات بما في ذلك أنظمة الاتصالات التي تدعم الصناعة، والمعاهد المختلفة أو السكان بشكل عام. والأمثلة على هذا هي: البنية الأساسية لمعلومات الشركات، والبنية الأساسية للمعلومات المالية، والبنية الأساسية لمعلومات الدفاع، والبنية الأساسية للمعلومات الكونية.

ويشير "حيز المعلومات" (Information Space) إلى التراكم المعلوماتي لكافة مصادر المعلومات التي تتوفر لجهة ما. فبالنسبة لشركة ما، يتضمن هذا التراكم المعلوماتي كلاً من البيانات التالية: الموظفين، والوثائق المطبوعة، ونظم أجهزة الكمبيوتر والاتصالات، إلى جانب كافة البيانات المشفرة الموجودة في بيئة تلك الشركة. وأما مصطلح "الحيز التخيلي"، فهو حيز المعلومات الإجمالية لكافة شبكات الكمبيوتر.

ويعمل الحيز المعلوماتي لمصلحة ما أثناء وقت الحرب فهو موقع المعركة والذي يشتمل على كل شيء في تلك البيئة، بما في ذلك إشارات الاتصال المنقولة في الجو. ويطلب كل جانب من الجوانب المتحاربة توسيع نطاق معرفته إلى الحد الأقصى عن موقع المعركة، بينما يحاول أن يحجب عن عدوه أكبر قدر ممكن من المعلومات وطرق الوصول إليها. وقد يحاول زرع معلومات مغلوطة لدى العدو، أو تخريب مصادر المعلومات التي يستخدمها العدو.

قيمة مصادر المعلومات

إن لمصادر المعلومات قيمة لدى الناس. كما أن لهذه القيمة مكونين أساسيين هما: قيمة تبادلية، وقيمة تشغيلية.

القيمة التبادلية. فتقررها قيمة السوق، وهي قيمة كمية يمكن تقييمها. وهي السعر الذي يمكن أن يدفعه شخص ما لمصدر معلومات محدد (1).

القيمة التشغيلية. يمكن تحديدها من الفوائد التي يمكن أن نجنيها من استخدامها. ويمكن أن تكون القيمة التشغيلية لمصادر المعلومات قابلة للتقدير الكمي، إلا أن هذا ليس دائماً. فعلى سبيل المثال، يمكن استخدام الكمبيوتر كوسيلة للتعلم، أو فتح المجال للحصول على وظيفة أفضل. وكذلك فإن المعلومات التي تتوفر عن مواقع قوات العدو، أو عن معالجة السرطان يمكن أن تنقذ كثيراً من الأرواح. كما يمكن الاستفادة من بحث علمي أو الاكتشافات الجديدة للحصول على ملايين أو مليارات الدولارات أحياناً، إذ يمكن إنشاء فرص عمل جديدة للعديدين، والمساهمة في الاقتصاد المحلي أو العالمي. كما أن الحصول على معلومات عن أسلحة كيميائية أو بيولوجية في بلد أجنبي قد يؤدي إلى إيقاف مثل تلك البرامج وإيقاف استخدام مثل تلك الأسلحة الفتاكة في المستقبل. ويصعب في مثل هذه الحالات تقدير قيمة كمية محددة مادياً عن الفوائد التي يمكن أن نجنيها من مثل هذه المصادر من مصادر المعلومات.

وتتفاوت قيمة مصادر المعلومات لجهة ما عن جهة أخرى. فقد تكون قيمة مصدر المعلومات لأحد الأطراف بمثابة نتيجة ناجمة عن ستة عوامل هي: 1ـ اهتماماته والتزاماته. 2ـ قدراته. 3ـ توفر مصدر المعلومات بالنسبة له. 4ـ توفر المصدر ذاته بالنسبة لخصمه. 5ـ تكامل مصدر المعلومات. 6ـ الوقت الذي تصل فيه المعلومات.

1- **اهتمامات هذا الطرف والتزاماته**. لنفترض على سبيل المثال أن متسللين ألمان تمكنوا من التسلل إلى الملفات الموجودة في كمبيوتر وزارة الدفاع الأمريكية أثناء حرب الخليج. فمن الواضح جداً أن هذه البيانات لها قيمة بالنسبة للجيش الأمريكي، وإلا لما أنشئت هذه الملفات في المقام الأول. فلو أن هذا المتسلل استطاع الحصول على هذه الملفات فمن المحتمل جداً أن تكون لها قيمة كبيرة للحكومة العراقية. ومع ذلك، فقد تكون هذه الملفات عديمة الفائدة لبائع فلافل. وأما بالنسبة للمتسللين أنفسهم، فإن الحصول على هذه الملفات أعطاهم، على الأقل، حقوق الافتخار على الناس

1- تلتقي هذه الفكرة مع فكرة هومانس في التبادلية الاجتماعية والمأخوذة من النظريات الاقتصادية بأن العلاقة المتبادلة بين الناس يتم تبادلها كالسلع ولها قيمة مادية أو معنوية وتخضع لقوانين الاقتصاد. وكذلك المعلومات هنا لها قيمة تبادلية بين (البائع والمشتري).

بقدراتهم والشعور بالرضى عن الذات وأنهم استطاعوا أن يهزموا ذلك النظام. ولو قدر لهؤلاء المتسللين أن يبيعوا هذه الملفات للعراق، أو إلى أية جهة أخرى فستكون هذه المعلومات ذات قيمة مادية بالنسبة لهم.

2- **قدرات الطرف الآخر على الاستفادة من المعلومات،** تتضمن هذه القدرات كلاً مما يلي: المعرفة، والقدرات والمهارات، والأدوات، وتستبعد إمكانية التوصل إلى مصدر المعلومات، وهذا ما يغطيه العامل الثالث. فعلى سبيل المثال، إن قرصاً يعني لمن يملك جهاز كمبيوتر أكثر بكثير مما يعني لشخص لا يملك جهاز حاسب. وكذلك الأمر، فإن معرفة الموقع الدقيق للقوات العراقية خلال حرب الخليج الثانية يعني الكثير للجيش الأمريكي الذي لديه القدرة على الاستفادة من هذه المعلومات واستغلالها والانتفاع بها، إذا ما قورنت بفائدتها لفرقة موسيقية مثلاً ليس لها أية معرفة أو قدرة على استغلال تلك المعلومات والاستفادة منها. وهكذا.

3- **توفر مصدر المعلومات للطرف المعني،** فهو مقياس درجة إمكانية التوصل إلى مصدر المعلومات بحيث يمكن استخدامه في أية طريقة مناسبة. ويتعلق توفر المعلومات بالسرية الخاصة بتلك المعلومات التي يجب أن تبقى سراً، وأن لا تتوافر لديه المعلومات، كما تتعلق بالمفهوم الأشمل، وهو أن الطرف المعني لا يمكنه استخدام تلك المعلومات واستخدام محتوياتها بطريقة أو بأخرى. ويتضمن هذا إمكانية استعراض المعلومات، أو معالجتها، أو تغييرها، أو نسخها، أو توزيعها أو بيعها.

وتتناسب قيمة مصدر المعلومات مباشرة مع توافره للطرف المعني. فملفات الجيش الأمريكي مثلاً، لن يكون لها أية قيمة بالنسبة للعراقيين طالما أنها لم تصل إليهم. فإذا حصل عليها العراقيون تصبح هذه الملفات ذات قيمة لهم. بل ستكون هذه الملفات ذات قيمة أكبر إذا استطاع العراقيون إملاء محتويات الملفات أو تغييرها دون أن يشعر أحد بهم.

4- **توفر مصدر المعلومات للأطراف الأخرى**. إن القيمة التشغيلية لمصادر المعلومات هي في سياق حرب المعلومات، فهي تتناسب عكسياً بتوافر مصدر المعلومات للأطراف الأخرى. فالملفات العسكرية كان يمكن أن تكون أقل أهمية للولايات المتحدة الأمريكية لو أنها بيعت إلى العراق. وفي مثل هذه الحالات، فإن قيمة المعلومات ترتبط جزئياً بتوفرها حصرياً، أي منعها عن يد الأعداء. وقد تأتي

قيمة مصدر المعلومات من ندرتها، فإذا كان الفرد هو الطرف الوحيد في هذه العملية، أو أحد قلة قليلة من الأطراف الذين يمكنهم التوصل إلى هذه المعلومات فإنه أهم بكثير من توافر المعلومات على نطاق واسع للجميع. وتزداد قيمة بعض مصادر المعلومات لدى توزيعها، فعلى سبيل المثال، فإن المنشورات التي وزعتها القوات المتحالفة أثناء حرب الخليج زادت قيمتها. وبهذا المحتوى، فإن قيمة مصدر المعلومات تستمد من استخدامه كوسيلة لاختراق فضاء المعلومات والأذهان للجنود العراقيين.

5- **تكامل المعلومات**: هذا مقياس تكامل المعلومات، أو جودة المصدر أو درجة دقتها وكمالها وأصالتها ومصداقيتها. وغالباً ما يتزاوج تكامل المعلومات، أو تُفسَّر بحيث يتضمن موثوقيتها، أي النوعية أو الحالة التي تؤكد أنها معلومات موثقة أو أصيلة، ولا يمكن إنكارها، أي أن الشخص لا يمكن أن ينكر أنه أرسل تلك المعلومات أو عالجها شخصياً. وبمعنى آخر: إن المعلومات التي تثبت أن الشخص المرسل أو المعالج غير مشكوك به ولا تحوم حوله الظنون والشبهات. وفي مثال حرب الخليج، فإن تكامل بيانات ملفات الكمبيوتر التي استطاع المتسللون التوصل إليها سيتم تحديده بمطابقتها للحقائق والوثائق الأخرى وبتوثيقها. فإذا لعب المتسللون ببيانات أي ملف من تلك الملفات فسيؤثر هذا على انقاص قيمة تكامليتها، وبالتالي، سيؤدي هذا خفض قيمتها بالنسبة للأمور العسكرية (أو على الأقل إلى أن تتم إعادة بيانات تلك الملفات إلى وضعيتها الأصلية قبل التحريف). كما أن قيمة مصدر معلومات ما بالنسبة للاعب قد تتناسب بشكل مباشر مع تكامليته ومصداقيته، إلا أن هذا ليس هو الحال في الغالب. فيمكن أن يفيدنا الخداع في هذه الحالة، وقد يستفيد لاعبٌ ما من تخريب وسيلة معلومات بشكل عالمي. فعلى سبيل المثال، يمكن اختراع قصص وتلفيقها بشكل كاذب ونشرها على الإنترنت.

6- **الوقت**: ويمكن أن تزداد قيمة المصدر أو تقل حسب دور مصدر المعلومات في العمليات. ففي حرب الخليج مثلاً، فإن المعلومات التي توفرت عن مواقع الصواريخ العراقية، وخاصة تلك التي تم إطلاقها ضد إسرائيل، كان يحتمل أن تكون هامة جداً من حيث الوقت. بينما يمكن أن تكون المعلومات عن مركز القيادة والتحكم العراقي أقل من أهمية بيانات المصدر المشار إليه عن الصواريخ العراقية. ويمكن التمييز بين القيمة الحقيقية والمحتملة لمصدر معلومات ما، فالقيمة الفعلية لمصدر المعلومات تشير إلى قيمته بالنسبة للطرف المعني قبل إجراء عملية حرب معلومات.

ثانياً : أطراف الصراع

هناك طرفان رئيسان في أي عملية من عمليات حرب المعلومات وهما: طرف الهجوم، وهو الذي يقوم بشن عملية ضد مصدر معلومات محدد، وطرف الدفاع، وهو الذي يهدف إلى المدافعة ضد تلك العملية، بالإضافة إلى الطرف الذي يقوم بدور مزدوج (هجوم ودفاع).

1ـ **الهجوم** : لقد كسبت قوات التحالف الحرب جزئياً بسبب عمليات حرب المعلومات. ويمكن أن يكون الأطراف على الجانبين كليهما أفراداً يعملون بشكل مستقل، أو في جماعات منظمة أو غير منظمة. ويمكن أن يكون هؤلاء الأفراد رسميين في الدولة أو غير رسميين. وقد يكون لهم من يكفلهم ويدعمهم أو لا يكون لهم من يكفلهم ويدعمهم. ويجب أن يكون لدى الطرف المعني النية، والوسائل، والفرصة كي يتمكن من الدخول في حرب المعلومات. فالنية هي نتيجة تلائم اهتمامات الطرف المعني والتزاماته. وأما الوسائل فيتم تحديدها بالقدرات وإمكانية الوصول (التوفر). وأما الفرصة، فهي وظيفة التوصل إلى المعلومات، إلا أنها تتضمن عوامل أخرى كتصور نجاح العملية وأن الشخص لن يتم إيقافه أو إلقاء القبض عليه. فإذا كانت إمكانية الوصول إلى المعلومات غير كافية من البداية فمن الضروري الحصول على وسيلة للوصول إلى المعلومات قبل محاول تحقيق أي هدف من الأهداف الأخرى. فعلى سبيل المثال، تخريب مصدر معلومات ما.

ومع العلم بأنه يمكن لأي فرد أو منظمة الانخراط في عملية حرب معلومات هجومية، إلا أن كثيراً من العمليات التي تحدث فعلاً إنما تنطوي تحت بضع فئات عامة. وتتضمن هذه الفئات ما يلي: عملاء داخليين (من داخل المؤسسة)، ومتسللين، ومجرمين، وشركات وحكومات وإرهابيين.

1ـ **الداخليون** (Insiders) : ويشمل كلاً من: الموظفين، والموظفين السابقين، والموظفين المؤقتين، والمقاولين وغيرهم ممن له صلاحية للدخول إلى داخل مباني المؤسسة المطلوبة ومصادر معلوماتها. وتُعد هذه الفئة بشكل عام أكبر تهديد للمؤسسة. ويعمل هؤلاء كوسطاء معلومات بحيث يبيعون المعلومات الحساسة التي تخص المؤسسة التي يعملون فيها أو لديها إلى حكومات أجنبية، أو إلى منافسين وإلى أتباع الجريمة المنظمة. وتشتمل أعمالهم التخريبية على سرقة وبيع مخططات وتصاميم

عسكرية وتجارية، وعمليات تجسس، وخرق الخصوصية الشخصية. ويمكن أن تقوم الفئة الداخلية بتخريب نظم المعلومات وأجهزة الكمبيوتر التي يملكها صاحب العمل، أو يهربون الأسرار التجارية للشركة لإنشاء شركات منافسة. وحتى إذا لم تكن هذه المصادر الداخلية مصدر الهجمة بذاتها، فيمكن أن يساعد هؤلاء الداخليون برغبتهم أو رغماً عنهم غيرهم من المعتدين. وقد تدفعهم الرشاوى المالية، أو المبادئ الإيديولوجية الفكرية، أو حب الانتقام والثأر، أو الرغبة بمساعدة أشخاص خارجيين يستغلونهم بطريقة أو أخرى.

2- **المتسللون (الدخلاء)** (Hackers): الدخيل هو الشخص الذي يتمكن من الوصول أو التعامل مع نظم إلكترونية، وبخاصة أجهزة حاسب وأجهزة الاتصالات بطريقة غير شرعية. وقد تكون الدوافع لهذا التسلل الحصول على اللذة والمتعة، أو الفوز في التحدي، أو تحصيل قوة أو شهرة. ومع العلم بأن كثيراً من المتسللين، وربما كلهم، لا يطلبون تحقيق جوائز مالية أو لا يرغبون بتخريب أجهزة الكمبيوتر التي يهاجمونها ويتسللون إليها، إلا أن هناك من يتسلل من أجل الحصول على الأموال أو تدمير أجهزة الكمبيوتر. ومع ذلك، فحتى عند عدم وجود نوايا شريرة لدى المتسللين فإن التسلل غير المصرح به يتسبب في تدمير تكاملية تلك النظم، وهو أكثر من مزعج لمالكي تلك النظم.

3- **المجرمون** (Criminals): وهم الذين يستهدفون المصادر المالية كالحسابات البنكية وبطاقات الائتمان أو الممتلكات الفكرية التي يمكن تحويلها إلى نقود من خلال المبيعات السرية المشبوهة. وغالباً ما يتعامل هؤلاء ضمن نطاق الجريمة المنظمة، إلا أن المجرمين من الأفراد أيضاً نجحوا في تنفيذ عمليات إجرامية حصلوا بنتيجتها على ملايين الدولارات. فالدافع الأساسي هو المال، والثروة. وتتضمن هذه المجموعة كلاً من وسطاء المعلومات أو السماسرة والأفراد الذين يبيعون البرامج المقرصنة والأقراص المدمجة التي تحتوي على برامج مختلفة ذات قيمة، وأشرطة الفيديو التي عليها مادة مسجلة ليست للبيع أصلاً.

4- **الشركات** (Corporations): هذه الشركات تنخرط في عمليات حرب معلومات هجومية عندما يتجسسون بنشاط على منافسيهم لسرقة أسرارهم التجارية

من خلال وسائل غير شرعية بإغراء أفراد داخليين لدى المنافسين بالرشاوى. فهؤلاء يبيعون معلومات عن عملائهم وزبائنهم، وقد يخترقون الحرية الشخصية والخصوصيات. ويدفع هؤلاء حب المال والمنافسة.

5- **الوكالات الحكومية** (Government Agencies): ينخرط عدد من الوكالات الحكومية في عمليات حرب معلومات هجومية. وتستهدف السلطات القانونية سجلات الاتصالات وهيكل المؤسسة للمجرمين للحصول على أدلة ومعلومات استخباراتية أثناء التحقيقات في وقائع الجرائم. وتطلب وكالة الاستخبارات كلاً من الأسرار العسكرية، والدبلوماسية، والأسرار الاقتصادية للحكومات الأجنبية، والشركات الأجنبية والأعداء الأجانب. وغالباً ما تركز الاستخبارات على المصادر الداخلية والمراقبة الإلكترونية لتوفير هذه المعلومات. وغالباً ما تدمر الوحدات الحربية قيادة الأركان والإدارة لدى الأعداء أثناء الحرب. ويراقب مسؤولون حكوميون رسميون الخطابة، وتقيد حرية الوصول إلى المعلومات والتعامل مع تقنيات المعلومات من أجل الحفاظ على الأمن الوطني وأهداف الأمن العام.

6- **الإرهابيون** (Terrorists): وهم على جانب خاص من الأهمية بسبب ما يمكن أن تلحقه هجماتهم من الأضرار على البنية التحتية الأساسية مثل: خدمات الطوارئ والنظم المالية وغيرها. ويجمع الإرهابيون معلومات عن أهدافهم، وينشرون الدعايات المغرضة والمشوشة، كما يخربون المعدات الفعلية والمباني. ولم يتم الإبلاغ إلا عن بضع هجمات على الفضاء التخيلي (عبر الإنترنت وشبكات الكمبيوتر) من قبل المخربين الإرهابيين، وهناك فئات أخرى غير التي ذكرت أعلاه منهم الأشخاص النشيطون سياسياً، والمتطرفون، والمتطفلون، والمخربون بشكل عام. ولا يمكن فصل هذه الفئات عن بعضها. فالمتسلل إلى أجهزة الكمبيوتر ونظم المعلومات مثلاً، يمكن أن يكون من الأفراد النشيطين سياسياً، أو قد يكون من الأشخاص الذين يعملون من داخل مؤسسة ما، أو من الإرهابيين أو جاسوساً لشركة ما.

2ـ الدفاع

يقوم كافة الفرقاء المعنيين باستخدام حرب المعلومات الدفاعية، سواء على مستوى الأفراد، أو المؤسسات أو الحكومات. فعلى مستوى الأفراد، يستخدم الدفاع لحماية

الخصوصية الخاصة، والمصادر الشخصية، والوظيفة المنافسة، والأحوال العامة بشكل عام. وأما على مستوى المؤسسات، فهي تستخدم للحفاظ على الوضعية المنافسة والمصادر الخاصة بتلك المؤسسة. وأما بالنسبة للحكومات، فهي تستخدم لحماية الأمن الوطني، والأمن الاقتصادي، والأمن العام، والنظام والقانون.

ويقع دور الحكومة في حرب المعلومات الدفاعية في عدة مناطق هي: الدفاع الوطني، وتأسيس الحمايات القانونية، وإرساء المقاييس، والبحث والتطوير عن تقنيات جديدة للدفاع. ففي الولايات المتحدة الأمريكية يتمتع مكتب التحقيقات الفدرالية بصلاحيات التحقيق في التجاوزات التي تحدث على القانون الفدرالي، وبالقيام بأعمال مضادة للتجسس وبتنسيق مثل هذه الأعمال في الولايات المتحدة الأمريكية، وأن يكون الساعد الأيمن للمدعي العام المسؤول عن تنسيق تطبيق القوانين الفدرالية المحلية المتعلقة بالأمن الوطني والجاهزية للطوارئ. وتعالج وزارة الخزينة بعض الجرائم المالية المحددة مثل موضوع تزوير بطاقات الائتمان، بينما تعالج الوكالات والمؤسسات القانونية الأخرى التحقيق في الجرائم المحلية. وأما مسؤولية الدفاع الوطني بما في ذلك عمليات الاستخبارات والاستطلاعات الأجنبية المضادة فتقع بشكل كبير على وزارة الدفاع.

3ـ الدور المزدوج

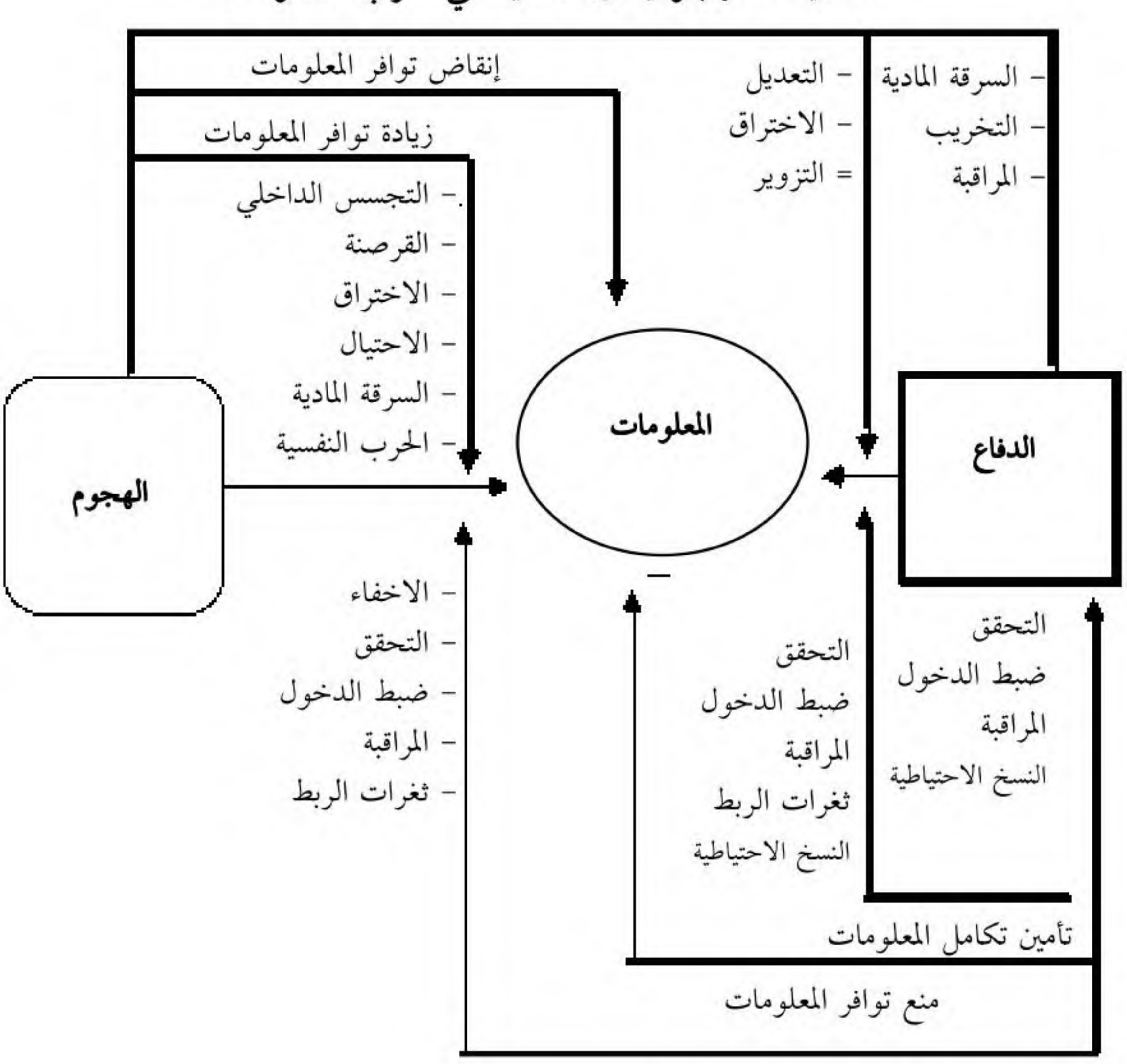
يمكن أن تلعب الجهات المشتركة في حرب المعلومات دوراً في العمليات الهجومية والدفاعية. فأثناء حرب الخليج مثلاً، أجرى الجيش الأمريكي عمليات حرب معلومات هجومية ودفاعية مدمراً، أو معطلاً مركز القيادة والأركان وأنظمته في العراق، بينما قام بالدفاع عن معلوماته.

وقد يتصارع الطرفان في بعض الحالات على الاستفادة من المعلومات من مصدر ما، ويقوم كل منهما بعمليات حرب معلومات هجومية ودفاعية. وتعتمد فائدة المعلومات على القيمة التي يمكن أن يستفيد منها كل من الطرفين من مصدر المعلومات، وهذا بالطبع يعتمد على أي الأطراف يستطيع التوصل إلى مصدر المعلومات ذاته بحرية أكثر. كما أن قدرات الطرف ذاته وإمكانياته هي الأخرى عامل هام. فقد يكون لأحد الطرفين درجة أقل من التوصل إلى المعلومات، إلا أنه يتمتع بمعرفة كبيرة، ومهارات فائقة، ولديه وسائل قوية فيمكن الاستفادة من تلك المعلومات بقدراته إلى درجة كبيرة لصالحه ويستفيد منها استفادة قصوى.

ويمكن تفسير المكاسب والخسائر الناجمة عن عملية هجوم في حرب المعلومات على مصدر ما حسب النتائج الثلاث التالية: زيادة توفير مصدر المعلومات للمهاجم، خفض توفير مصدر المعلومات بالنسبة للمدافع، وخفض تكاملية مصدر المعلومات. وهذه النتائج جميعها تزيد قيمة مصدر المعلومات بالنسبة للمهاجم وتخفض قيمته بالنسبة للمدافع، والشكل التالي يبين ذلك.

شكل رقم (4)

العمليات الهجومية والدفاعية في حرب المعلومات



المصدر : Denning, 2000 b, p. 13.

وقد تتسبب كثير من العمليات بآثار متعددة، وخاصة العمليات التي تتم خلال فترة زمنية طويلة وتتناول عدة مصادر معلومات. وبغض النظر عن هذا، فمن المستحسن أن نأخذ هذه الآثار كلاً على حدة، إذ أن كلاً منها يوفر طريقة تصنيف ومقارنة لمختلف أنواع العمليات.

الإعداد والتصميم في حرب المعلومات

إن معرفة إمكانيات الخصم عامل هام في تخطيط المعركة وعامل حاسم في الكسب أو الخسارة، وقديما فإن عنصري المباغتة والتكتم يشملان استغلال المعلومات لصالح ذلك الطرف والأمثلة التاريخية كثيرة في استخدام وسائل حرب المعلومات في المعارك، فالمسلمون قد استخدموا إشعال النيران في فتح مكة لإيهام العدو بالكثرة الساحقة لهم، وكانوا يستنبطون المعلومات من الجواسيس والمارة عن حجم الخصم. واستخدام المرايا والتنصت والتموية والرعب والإخافة ... إلخ كل هذه تعد من وسائل الاستفادة من المعلومات، أو استغلالها، أو التأثير من خلالها على معنويات الخصم. كما أن انتقاء معلومات الخصم وتمرير اتجاهاته وتحليلاته وقراءته كبديل عن المواجهة المباشرة، مما يزيد على معنوياته ويربك خططه ويجعله يشعر بأنه مكشوف وأنه في خطر، هذا بالاضافة إلى استخدام أدوات تخريب المعلومات (كالفيروسات).

نمذجة حرب المعلومات

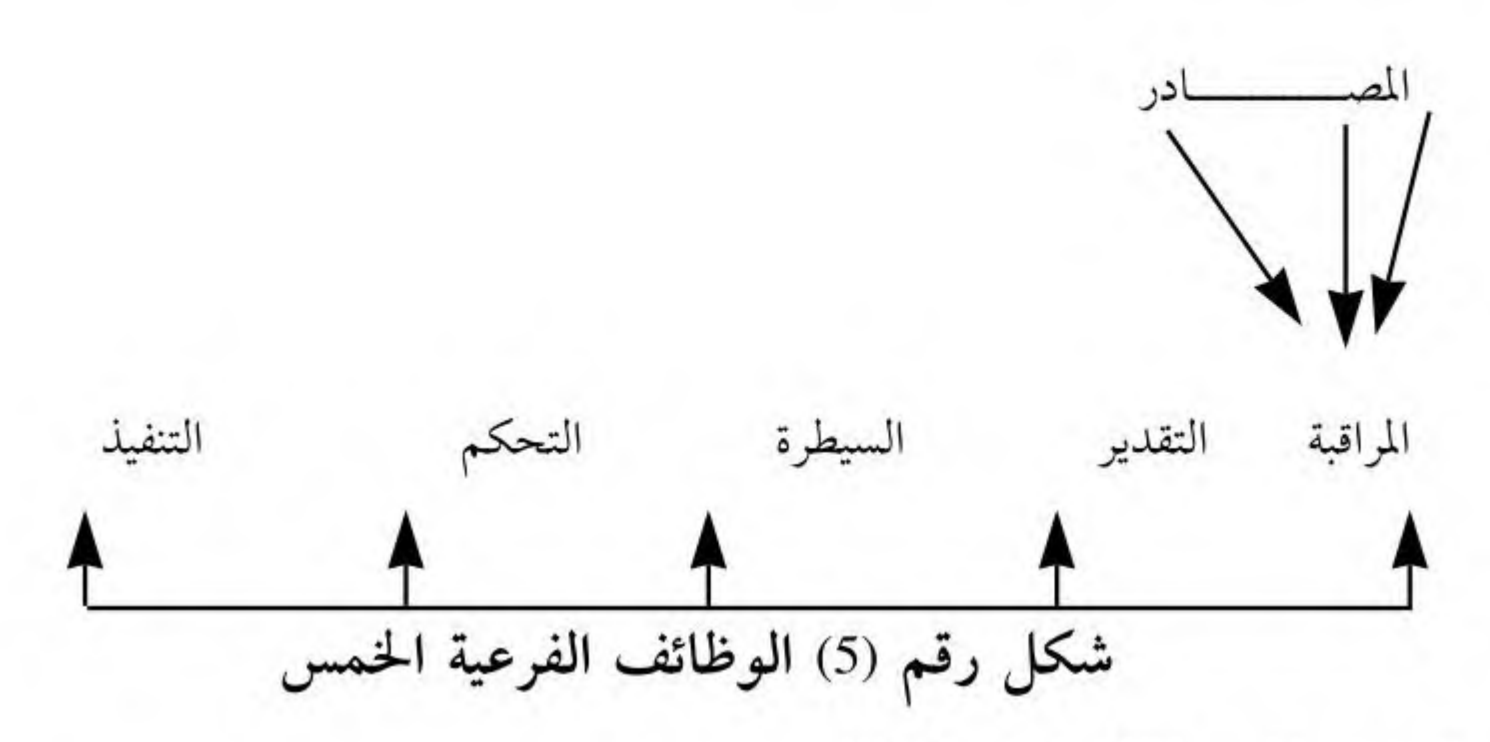
كثيرٌ من الناس يحتار في أي نوع حاسب يشتري، فالبعض يقول أريد حاسباً حديثاً، أو ذا شاشة ملونة، أو سرعة عالية ... والسؤال البديهي هو ما الاحتياجات؟ لكي تتم المواءمة بين الاحتياجات والمواصفات. وهذه الفكرة الأساسية هامة عند تصميم أنموذج لحرب المعلومات، وبمعنى مالذي لدى الخصم من مكونات معلوماتية؟ فلابد من تحليل المعطيات بطريقة نظام (System)، وذلك للمساعدة في التخطيط والتنفيذ والدفاع ضد حرب المعلومات. ان من المهم تحديد مركز الجاذبية عند الخصم (COG) وعندنا، وتحليل النظام ونمذجته يتطلب تحديد المشكلة والهدف من الأنموذج، وأهدافه، وحدوده، والاتجاه الكلي للأنموذج «التصور العـــــام» (Okello, et. al., 1996).

ولتخطيط حرب المعلومات لابد من أخذ عدد من الأبعاد التي تكون في مجملها حرب المعلومات، ويستخدم مفهوم الأبنية العملياتية (Operational Architectures)

للإشــارة إلى النمــاذج التي تـصف سلوك الـنظام (System) والتي يمكـن أن تحلل إلى خمسة مكونات هي : (الوظيفي (Functional)، والعملياتي الساكنة (Operational Static)، والبيــانات / المعلومــاتي (Data/Informational)، والعــمليــاتي الديـنامي (Operational Dynamic).

أن المكون الوظيفي يصف المهام الواجب تنفيذها والأقفال الداخلية اللازمة، أما المكون المادي فيصف المكونات اللازمة للنظام واتصالاتها (الارتباطات المتبادلة للمكونات). في حين ترسم العمليات الساكنة المهام لكل عملية محددة، وتحدد البيانات كمكون البناء المعلوماتي اللازم وأخيراً تنفذ العمليات الديناميـة الأنموذج المستخدم لتحليل أداء النظام.

ويحلل أوكيلو وزملائه (Okello, et. al, 1996) الأبنية العملياتية إلى خمس وظائف هي المسح أو المراقبــة (Survey)، والتــقــديـر (Assess)، والســيطرة (Command)، والتـحكم (Controal)، التنفيـذ (Exective)، ويمكن تطبيق هذه المكونات على البناء المادي. ولابد من تحقيق الوظائف الفرعية في أي مرحلة حرب معلومات، والشكل التالي بين ذلك.



شكل رقم (5) الوظائف الفرعية الخمس

المصدر: .Okello, et.al., 1996, p. 43.

فالمراقبة أول هذه الوظائف والتي تسعى إلى جمع المعلومات والبيانات عن الخصم، أما التقدير فيرجع إلى هضم المعلومات الكثيرة والتي يمكن الحصول عليها من الستالايت ويمكن جمع المعلومات من مصادر مختلفة منها التجسس الإلكتروني

والبشري وتجسس الإشارات، والتجسس القياسي والتوقيع والتجسس الفني، والتجسس المضاد وتجسس المصادر المفتوحة. أما وظيفة التقدير (Assess). هنا يتم صهر المعلومات وهضمها ودمجها وتحويلها إلى صورة معركة فضائية . أما وظيفة السيطرة (Command) فهي تلقي صورة المعركة من وظيفة التقدير، والتخطيط وتحديد نوعية الفعل المطلوب. أما وظيفة التحكم (Control) يحلل هنا طلبات المهمات والتقديرات الجاهزة والاستجابة للتهديدات والتغيرات الموقفية وتقديم النتائج للخلف وفق تسلل القوة، وأخير التنفيذ (Excute)، ويشمل التنفيذ هجوم المعلومات والدفاع عن المعلومات ووسائل التنفيذ هنا تشمل الهجوم والدفاع وبغض النظر عن الطريقة المستخدمة.

عمليات الدفاع والهجوم المعلوماتي

هناك ست فئات من عمليات الدفاع والهجوم المعلوماتي وهي :

1- العلميات النفسية (Psychological Operations).

2-الحرب الإلكترونية (Electronic Warfare).

3- الخداع العسكري (Military Deception).

4- التدمير المادي (Physical Destruction).

5- الإجراءات الأمنية (Security Measures).

6- الهجوم المعلوماتي (Information Attack).

1- العلميات النفسية (Psychological Operations).

هناك أقسام متخصصة في العمليات النفسية خلال السلم والحرب مثل (MC-130E) في الولايات المتحدة الأمريكية والتي كان لها دور كبير في عملية عاصفة الصحراء من خلال المنشورات واستعراض القوة، وتمت مناقشة هذه العمليات لاحقاً بالتفصيل

2- الحرب الإلكترونية (Electronic Warfare).

يشترك الكثير من الأدوات الكهربائية والمعدات كالحاسب وغيره بالمجالات الكهرومغناطيسية، وأحد مجالات حرب المعلومات هو تدمير أو تعطيل هذه المجالات

كما يعني تعطيل الكثير من الاتصالات (الحاسب، الإنترنت، الفاكس، الجوال . . . إلخ.). كما أن من استخدام النبضات الكهرومغناطيسية (EMP) وهو ما تحدثه التفجيرات النووية وبشكل ضخم جداً، ولكن تصاميم مصغرة من هذه النبضات تعطل أبراج الاتصالات ومحطات الطاقة.

3- الخداع العسكري (Military Deception).

يُعد الخداع العسكري أحد العمليات النفسية الأخرى الهامة في حرب المعلومات فيمكن استخدام ذلك للتأثير على معنويات وإدراك الخصم أو لتوجيه انتباهه إلى موضوع آخر.

4- التدمير المادي (Physical Destruction).

ويقصد بالتدمير المادي السريع المضاد للرادارات، وقنابل (HARM)، و (AGM-65)، مافريك (Maverick)، و(G BU-15). كما أن استخدام نظم الكهروميكانيكية (MEMS).

5- الإجراءات الأمنية (Security Measures).

هناك عدد من الإجراءات الدفاعية والهجومية المتعلقة بحرب المعلومات. إن حفظ المعلومات الاستراتيجية وكلمات السر والعمليات والبرامج خطورة هامة تجعل الحصول على المعلومات عملية صعبة ولكن غير مستحيلة، ومن وسائل الحماية هذه التشفير وجدران الحماية.

6- الهجوم المعلوماتي (Information Attack).

يمكن أن يحصل هجوم على المعلومات لاغراض متنوعة منها استغلال المعلومات أو الحرمان من استخدامها أو تخريبها، أو تدميرها، أو تحويرها. ومن الأمثلة على ذلك الدخول غير المصرح به والقرصنة والمتطفلون. . .إلخ.

خطوات تنفيذ حرب المعلومات

إن القيام بحرب المعلومات سواء كان بقصد الدفاع أو الهجوم يتطلب التخطيط مثل أي حملة أخرى،إنها تتطلب أن يعرف الطرف نفسه ويعرف خصمه، ويعرف

نفسه للدفاع المثالي عنها، ويعرف خصمه للهجوم المثالي عليه، ولابد من تحديد الأهداف من وراء أية حملة هجوم أو دفاع معلوماتي وتحديد هذه الأهداف بشكل واضح، عندما يفهم النظام وتحدد الأهداف ويُختار الأفراد المناسبون لتحقيق الأثر المنشود، وفيما يلي ملخص للخطوات اللازمة لحرب المعلومات:

1- **حلل النظام** (Analyze the System). إن أول خطوة في حماية المعلومات أو الهجوم على معلومات الخصم هو تحليل النظام، والهدف هو تحديد العناصر والعقد الخاصة بالنظام والارتباطات بينها، ولابد من تقييم وظائف النظام مكان التحليل، ومطابقة النظم المادية مع المجالات المتنوعة للوظائف، وإن النتائج الناجمة عن هذا التكامل توفر البنية العملياتية الثابتة للنظام وتؤدي إلى فهم النظام عامة. والنظام عادة دينامي من خلال البيانات والمعلومات والطرق والبروتوكولات لنقل البيانات فيه، وهنا يمكن فهم النظام بحالته الدينامية، وفحص النظام الدينامي يؤدي إلى تحديد الثغرات ومداها وحمايتها في حالة الدفاع.

2- **قيم الأهداف** (Evaluate Objectives). هناك أهداف سياسية لحرب المعلومات وهنا لابد من فهم هذه الأهداف وتحويلها إلى أهداف عسكرية، ولابد من تحديد مركز الجاذبية بالنسبة لجميع العلميات أي النقطة التي تتمحور عندها جميع العمليات وترتبط بها بالنظر إلى الأهداف. وفي حالة الهجوم يتمركز الهدف حول تحديد العقد الحساسة والارتباطات في نظم العدو بحيث عند الهجوم يمكن تحقيق الأهداف.

3- **اختيار الأدوات** (Select Tools). في هذه الخطوة لابد من اختيار الأداة أو الأدوات المناسبة بناءً على عدة عوامل منها : مدى توافر الأداة لأنه ليست جميع الأدوات متوافرة في حرب المعلومات، بعض هذه الأدوات تحفظ لأغراض لاحقة أو لأسباب معينة، وغالبية الأدوات المتاحة على المستوى الاستراتيجي أو العملياتي لا تكون كذلك على المستوى التكتيكي. وهناك لابد من تحديد الأداة المناسبة والمتوافرة الآن وهنا (في هذا الموقف). كما أن مدى تحقيق الهدف عامل آخر في اختيار الأداة، بمعنى ماذا يريد المخطط أن يحقق من استخدام هذه الأداة؟ كما أن تقييم الهدف عامل آخر في تحديد الأداة المناسبة. وتحديد الأثر المرغوب إحداثه في الهدف الخصم، وهذه الخطوات هي ذاتها في حالة الدفاع المعلوماتي والفرق هو في الأهداف فقط.

وذكرت مجلة تايمز (Times) عن الحرب الفضائية (Cyber War) أنها تشمل حرب لوحة المفاتيح والفأرة وفيروسات الحاسب، ويمكن أن يتكون هجوم معلوماتي من العمليات التالية:

1- النبضات الكهرومغناطيسية، حيث يتم تسلل أي شخص إلى عاصمة العدو ويفجر قنابل من القنابل المبنية على النبضات الكهرومغناطيسية (EMP) مما يؤدي إلى خرق نظم الاتصالات والمال والبنوك وتعطيل الجوال والهاتف والفاكس . . . إلخ.

2- الفيروسات والديدان والميكروبات يمكن إمطار نظم الخصم بالفيروسات بكافة أنواعها وبالديدان والميكروبات الإلكترونية والتي تشل النظام والتطبيقات وتتكاثر بسرعة كبيرة مولدة أوبئة إلكترونية، وتغير مسارات التزويد، والمطارات، والانتهاء بشحن مواد غير مطلوبة وإرسالها إلى أمكنة فيزيقية.

3- التشويش والإعاقة والتخريب يمكن التشويش على اتصالات الخصم وإعاقتها من البث وتخريبها، وتزويدها بمعلومات مربكة ومظللة.

4- العمليات النفسية يمكن استخدام عدد كبير من العمليات النفسية الموجة للقادة وخاصة العسكريين والسياسيين وإلى عامة الناس وإضعاف روحهم المعنوية والتأثير على دعمهم وقناعتهم بسياسات بلدهم.

ولك أن تتخيل عسكري الغد وهو مزود بشريحة لتحديد موقعه مع نظام تحديد الموقع الجغرافي (GPS) ويمكنه من الرؤية الليلية، وبهاتف اتصال دولي، ودرع واقٍ ضد الكيماويات والأسلحة البيولوجية.

4- قييم الآثار (Assess Effects). وفي هذه الخطوة تتم مقارنة الآثار الفعلية مع الآثار المرغوب إحداثها في النظام الهدف (النظام المراد حمايته أو تدميره)، وهنا يمكن أن يعدل المخطط من أفعاله إذا لزم الأمر ويمكن إعادة الهجوم لتقييم الخطوات اللازمة لتقدير الأثر.

ويرى البيرتز (Alberts) أن حيز المعركة المرتبط بحرب المعلومات متحرك وممتد لما هو أكثرمن المواقف العسكرية التقليدية، وينظر له أحياناً على أنه استخدام المعلومات الذي يؤدي إلى فاعلية وفعالية. وهذا الاستخدام لحرب المعلومات قد أدى إلى المزيد من الغموض، لهذا السبب فإن استخدام مفهوم «استراتيجيات المعلومات» للإشارة إلى الاستفادة من المعلومات وتقديرها وتقنيات المعلومات كأداة في القوة الوطنية والتي يمكن أن تكون متصلة مع أو مرافقة إلى للوجود العسكري والعمليات.

الفصل السادس

حرب الخليج وأسلحة التخريب الشامل

مقدمة

لقد تنبأ نيكسون (1980) في كتابه «الحرب الحقيقية» بأن منطقة الخليج العربي منطقة بالغة الأهمية في المستقبل، ويقول علينا أن نعلم من يسيطر على ماذا في الخليج العربي والشرق الأوسط لأنه المفتاح الذي يسمح لنا بأن نعرف من يسيطر على ماذا في العالم، ويمثل العراق . . . أعظم قوة عسكرية في الخليج. لقد حل خلافاته الحدودية مع الكويت لكنه من المحتمل أن يخبئ المستقبل مشكلات إضافية. ونيكسون كما هو الغرب يرى الخليج من خلال النفط والصعاليك والثروة، حيث يشبه ذلك بالاستعارة التالية التي يستشهد بها لإحدى الشخصيات الأمريكية . . . سيدة ثرية تعيش بمفردها في مدينة صغيرة محاطة بالصعاليك. الجميع يعلم بأنها تملك ملايين الدولارات من الماس تحت سريرها ولا يوجد شرطة تحميها ومن حين لآخر يأتي مدير الشرطة (الشريف) يترجل ويطبع قبلة على خدها ثم يعود مسرعاً. فهل ستشعر بالأمان؟ هذه هي الصورة التي يحملها الغرب عن العرب، حيث تقوم الولايات المتحدة الأمريكية بدور «الشريف» الذي يطمئن السيدة، وبالتالي يقترح نيكسون الحاجة إلى الوجود الدائم للقوات الأمريكية من أجل حماية المنطقة من الصعاليك (الخليفة، 2000).

هل حرب الخليج حرب معلومات؟ أم هل كان للمعلومات دور كبير فيها؟ إن القول إن حرب الخليج حرب معلومات ينطلق من فعالية المعلومات في حسم الصراع، فمن يملك المعلومة يملك القوة، ومن يعطل المعلومة لدى الطرف الآخر يملك القوة، ومن يدمر البناء التحتي المعلوماتي يملك ميزات اضافية تمكنه من حسم المعركة. تعد حرب الخليج أول حرب معلوماتي تستخدم فيها الأسلحة الذكية بكثافة وتم ربط أكثر من (3000) حاسب في منطقة القتال مع الحاسبات المركزية في الولايات المتحدة.

ويرى كامبن أن عاصفة الصحراء تعد أول حرب معلومات بالمعنى الحديث لحرب المعلومات (Campen, 1992). يرى بودرلاد (Baudrillard) أن حرب الخليج الثانية حرب يمكن وصفها بأنها حرب لم تحدث، أو لا حرب (Non-Ward)، وهذا ناتج عن تطبيق التقنيات الحديثة في الحرب (Baudrillard, 1995).

إن استخدام المعلومات في الحروب ليس بالجديد، ولكن زيادة الاعتمادية على نظم المعلومات والمعلومات أصبح من سمات الصراعات في هذا العصر، وهناك أنواع

عديدة من عمليات حرب المعلومات استخدمت في حرب الخليج منها : التسلل إلى أجهزة الكمبيوتر، والتجسس البشري، والتجسس عن طريق الأقمار الصناعية، والمراقبة باستخدام آلات التصوير، والحرب الإلكترونية، والتخريب الفعلي لمواقع الاتصالات، وتزوير الأوراق، والإدارة النفسية، والعمليات النفسية، وكذبة فيروس الكمبيوتر. كما أن هناك المزيد مثل سرقة الأسرار التجارية، والتعدي على الأمور الشخصية، وتزوير البريد الإلكتروني.

وتبعاً للظروف، فإن بعض هذه الأعمال هي إجرامية، وبعضها الآخر غير قانوني، إن لم يكن غير أخلاقي، في حين يعتبر بعضها الآخر أعمالاً مقبولة من الحكومات. وإن بعض هذه العمليات مرتبط بالصراعات العسكرية، وبعضها الآخر على مستوى الأفراد، والمؤسسات أو المجتمعات، والقاسم المشترك الأعظم الذي يجمع فيما بينهما جميعاً هو أنها جميعها تحاول استغلال مصادر المعلومات لصالح المستفيد وضد الخصم. وفيما يلي استعراض لأهم أساليب حرب المعلومات التي استخدمت في حرب الخليج ومنها:

1- تدمير البناء التحتي المعلوماتي.
2- الوصول غير المصرح به.
3- التجسس العسكري المعلوماتي.
4- التجسس الإلكتروني.
5- زرع الفيروسات في نظم المعلومات.
6- العمليات النفسية.
7- الرقابة الإعلامية.

1- تدمير البناء التحتي المعلوماتي

أ. تدمير نظم المعلومات

قامت قوات التحالف بتحييد، أو تدمير النظم الرئيسة العراقية للمعلومات وذلك باستخدام الأسلحة الإلكترونية والعادية. وخلال اللحظات الأولى من عملية عاصفة الصحراء قامت طائرات مروحية، هيلوكبتر، والطائرات العادية وأسلحة مضادة

للإشعاع الذري بإطلاق "غيوم" عطلت شبكة الدفاع العراقية. كما تسببت أشرطة الدخان من ألياف الكربون فوق مقاسم الطاقة الكهربائية العراقية التي تمَّ إطلاقها من صواريخ طائرات التوماهوك بإحداث تماس كهربائي أدى إلى توقف مؤقت وانقطاع شامل للتيار الكهربائي في أنظمة الطاقة الكهربائية. كما استطاعت قاذفة مقاتلة في القوات الجوية الأمريكية من طراز (إف-117) من نوع ستيلث توجيه قذيفة دقيقة التوجيه لتسقط في عمود التكييف مباشرة في نظام الهاتف العراقي في مركز مدينة بغداد، مسببة فصل نظام الكبل المحوري الأرضي، والذي كان يربط ما بين الإدارة العليا للقوات العراقية مع العناصر المقاتلة المختلفة التي تعمل تحت قيادتها. وقد أدى هذا إلى قطع وسيلة الاتصال الأساسية بين مركز القيادة في بغداد ومختلف القوات في أرض المعركة. وبعد أن أصبحت القيادة ومركز التحكم عاطلين عن العمل، بدأت قوات التحالف توجيه ضرباتها لأنظمة الرادار العراقية بحيث شلت قدرتها على رؤية مواقع المعركة. وهكذا، بعد أن أصبح العراق "أعمى" و "أطرش" لم يعد لديه سوى فرصة ضئيلة جداً في النصر (Denning, 2000 b).

ب. شبكات الطاقة (The Power Grids) :

شبكات الطاقة مثلها مثل شبكات الهاتف معرضة للتخريب والتعطيل بالصدفة وبالعمد. إن فشل تشغيل هذه المحطات يشكل تهديداً أمنياً، إن تضليل (تعتيم) المدن قصداً يؤدي إلى خسارة اقتصادية كبيرة ومن الممكن أن يؤدي إلى فوضى لدى جمهور الناس ومظاهرات وأعمال شغب ... إلخ. ولا غرابة في تهديد إسرائيل المستمر للبنان بضرب البنى التحتية وخاصة شبكات الكهرباء والتي تم تدميرها فعلاً. أما على مستوى بلد مثل الولايات المتحدة وهي المكونة من أربع شبكات طاقة رئيسة تزود تكساس والولايات الشرقية والوسطى والولايات الشمالية الغربية وجميع هذه الشبكات مترابطة ومتصلة وتلتقي في نبراسكا، وجميعها مصممة وتعمل بالحاسب ويمكن أن يتوقف عملها جزئياً في المنطقة التي يسجل فيها خطأ واحد وتبقى المنطقة المحيطة بمنطقة الخطأ مضاءة.

ج ـ القنابل الكهرومغناطيسية

استخدمت قنابل من نوع (EMP/T) قنابل إرسال النبض الكهرومغناطيسي في بداية حرب الخليج لتدمير وتعطيل نظم الاتصالات العراقية بما في ذلك أسلحة الدفاع الجوي ومراكز التحكم والسيطرة. حيث استهدفت البحرية الأمريكية موقعين عراقيين للدفاع الجوي في جنوب العراق، حيث أطلقت هذه القنبلة على صاروخ كروز بالقرب من محطات الدفاع وعلى الفور اختفت الأضواء واختفت شاشات الرادار وتعطلت الكهرباء والاتصالات مع بغداد وانصرفت الجهود في البحث عن الخلل وفي هذا الوقت أطلق صواريخ كروز على فندق الرشيد وقامت طائرات (إف 117) بتدمير مصانع عسكرية.

2- الوصول غير المصرح به للمعلومات

لقد تمكن الدخلاء من الولوج إلى أحد النظم الخاصة بالعمليات العسكرية في عاصفة الصحراء قبل حرب الخليج، وتم نسخ ملفات وتغيير في ميزات الدخول ليتمكنوا من الدخول المستقبلي. ولقد كان الدخلاء يبحثون عن معلومات عن الأسلحة النووية.

لقد استطاع خمسة متسللين من هولندا التسلل ما بين عامي 1990-1991، إلى (34) أربعة وثلاثين نظاماً من أنظمة الكمبيوتر في مواقع الجيش الأمريكي على الإنترنت، بما في ذلك المواقع التي كانت موجهة مباشرة لعملية عاصفة الصحراء/ درع الصحراء. واستطاعوا تصفح الملفات فيها، والبريد الإلكتروني، والبحث عن الكلمات الأساسية مثل: نووي، أسلحة، صواريخ، درع الصحراء، وعاصفة الصحراء. واستطاعوا الحصول على معلومات عن مواقع دقيقة للقوات الأمريكية، وأنواع الأسلحة التي تمتلكها تلك القوات، وقدرة صواريخ باتريوت، وحركة السفن الحربية الأمريكية في منطقة الخليج.

وأفاد تقرير اخبار (ال آي ب. سي. .A.B.C) بأن الدخلاء كانوا يعملون لمدة لا تقل عن السنة، ويقرأون معلومات عسكرية حساسة حول الخطط العسكرية. ولقد تبين حصول الدخلاء على معلومات هامة عن صواريخ الباتريوت، وفي إحدى المراحل قاموا بغلق حاسبات في وسكانسون وفرجينيا والتي استخدمت لاحقاً في حركة الجيش في حرب عاصفة الصحراء. والمعلومات التي جمعت عن أطلاق

صواريخ الباتريوت وصورايخ البحرية توماهوك ودعوة الاحتياط. ولقد توقع المحققون أن يكون وراء هؤلاء الدخلاء الاستخبارات الروسية (KGB)، أو العراق ولكن لم يثبت ذلك (ABC News, 1991). وبعد أن انتهوا من الحصول على ما أرادوه، مسحوا كل آثار أنشطتهم من سجلات تلك الأنظمة وذلك في محاولة لإخفاء تسللهم.

ووفق ما أدلى به جيم كريستي (Christy)، مدير برنامج التحقيق في جرائم الكمبيوتر وحرب المعلومات في مكتب القاعدة الجوية للتحقيقات الخاصة، فقد استهدف هؤلاء المتسللون أنظمة التزويد العسكرية. ويقول كريستي "إنهم لم يفعلوا، ولكنهم كانوا قادرين على أن يطلبوا إرسال "فراشي أسنان" بدلاً من "طلقات الرصاص" إلى الخليج" (Smith, 1997).

إن الوصول لمعلومات تهدد حياة الجنود الأمريكان يعني أن الولايات المتحدة غير قادرة على حماية معلومات عساكرها الذين يحاربون باسمها، وقد تستخدم المعلومات ضد أسرهم. ولقد تمكن الدخلاء من تحديد تغيرات في هذه النظم والتي تمكنهم من دخلوها، ولقد تمكنوا من تعديلها ونسخ معلومات عسكرية هامة منها (Bowman, 1994).

ويقول شولتز (Schultz)، الذي كان مديراً لقسم الإبلاغ عن حوادث قدرة طاقة الكمبيوتر: "لقد كان لدى المتسللين قدر كبير من المعلومات والبيانات بحيث كان باستطاعتهم أن يملؤوا أسطوانات الأجهزة التي كانوا ينطلقون منها لتنفيذ أعمال التسلل التي كانوا يقومون بها. كما استطاعوا ملء عدد من الأسطوانات المرنة بالمعلومات والبيانات التي حصلوا عليها نتيجة لتسللهم. وعندما لم يجدوا متسعاً للبيانات التي حصلوا عليها نتيجة سرقاتهم اخترقوا أجهزة الكمبيوتر في جامعة "بولينغ جرين" وجامعة شيكاغو وحملوا تلك المعلومات عليها إذ اعتقدوا أنهم سيتمكنون لاحقاً من نقل تلك البيانات إلى أماكن أخرى (موثق في Denning, 2000 b, p. 3-4).

وتدعي بعض المصادر أن متسللين هولنديين حاولوا بيع المعلومات التي سرقوها إلى العراق أثناء حرب الخليج. ويقول شولتز: "إنه أبلغ هيئة الإذاعة البريطانية بأنه تلقى معلومات من مسؤولين حكوميين أن العراق عرضت عليه تلك المعلومات من خلال وسيط يعمل لحساب المتسللين." وأضاف شولتز أن بغداد رفضت هذا العرض خشية أن يكون هذا مقلباً أو فخاً لهم، كما أدلى المسؤول".

ويقول شولتز: "مع أنه تمَّ تحديد هؤلاء المتسللين ومعرفتهم، إلا أن الولايات المتحدة كانت عاجزة عن أن تقوم بأي عمل على الإطلاق حيال هذا الأمر، إذ لم تكن أعمال التسلل إلى شبكات الكمبيوتر غير قانونية في هولندا في ذلك الوقت. وقد كادت تنجح جهود ضباط مكتب التحقيق الفيدرالي الأمريكي بإغراء المتسلل المهاجم الرئيسي لإحضاره إلى الولايات المتحدة الأمريكية في مقابلة مدبرة مع شركة فضاء كبرى في ولاية فلوريدا، إلا أن المتسلل رفض العرض في آخر لحظة. وقد انتهى اثنان من المتسللين الخمسة إلى الحبس خلف القضبان في نهاية الأمر، ولكن هذا الحبس لم يكن بناء على "الغزو" الذي قام به ضد القوات العسكرية الأمريكية، بل بسبب عمليات تزوير للبطاقات الائتمانية (Browning, 1997).

3- التجسس العسكري المعلوماتي

كان للعراق اتصال بجواسيس داخليين. ففي شهر أيار/مايو 1991 تمَّ الحكم بالسجن لمدة خمس سنوات على المدعو جيورجن محمد جيتلر، وعمره 42 عاماً، ويعمل في قسم الأرشيف في وزارة الخارجية الألمانية بسبب تسريبه معلومات عسكرية وسياسية إلى العراق عشية حرب الخليج. ولقد سلَّم جيتلر المخابرات العراقية في بون مئات الوثائق قبل اعتقاله، واشتملت هذه الوثائق على رسائل من الرئيس الأمريكي جورج بوش إلى المستشار الألماني هلمت كول تتعلق بالخطط العسكرية لنقل مقاتلين وأسلحة من خلال ألمانيا. ووصفت التقارير أن وكالة المخابرات الغربية قدّرت ما عرفته عن الشركات الأجنبية التي تساعد العراق في بناء أسلحة الدمار الشامل، والتقديرات السرية الموثوقة عن العراق التي قدمتها وزارة الخارجية الأمريكية ومن حلف الناتو، وكذلك تقارير ألمانية عن الصواريخ العراقية والخرائط التي تبين مواقع تلك الصواريخ والأهداف المحتملة التي يريدون قصفها في إسرائيل. كما كان فيها أيضاً صور فضائية بالأقمار الصناعية تبين مواقع الصواريخ الإسرائيلية، وقائمة بعدد طائرات "الشبح" الأمريكية القاذفة التي سيتمّ نقلها إلى منطقة دول الخليج. وبعد أن توصلت المحكمة إلى اتخاذ قرار بأن هذا الشخص الذي هرَّب هذه البيانات هو "مذنب"، أصدرت محكمة دوسيلدورف بأن عملية التجسس العسكرية المفيدة التي قام بها المتهم قدمت للعراق "فوائد كبيرة" (Kirschbaum, 1997).

ويقول جيلتر بعد انتهاء مدة حكمه لخمس سنوات في مقابلة مع CBSفي برنامج "ستون دقيقة" إن تقديم أسرار الحلفاء إلى العراق إنما كان "متعة له، يقوم بها خمسة أيام كل أسبوع". كما قال أيضاً: "إنه كان يتلقى أجراً على تجسسه، ولكن هذا الأجر لم يكن الدافع الحقيقي لقيامه بهذا العمل". وأضاف قائلاً: "لقد كنت مع الجانب العراقي". و "لقد شعرت بأن هذا واجبي". وبعد مقابلة الملحق العسكري العراقي اللواء عصمت جودي محمد مصادفة في مطعم، تطوع جيلتر بتزويد العراق بالمعلومات. وتمَّ إلقاء القبض على جيلتر بعد أن قام الضباط الألمان المناوئون للتجسس باعتراض مكالمة هاتفية للواء عصمت (Associated Press, 1998).

وقد تابعت العراق أنشطتها التجسسية. ففي شهر تشرين الثاني/ نوفمبر من عام 1997 أبلغ مسؤولون عسكريون ومسؤولون في المخابرات الأمريكية أن عملاء استخبارات عراقيين نجحوا بالتجسس على مفتشي أسلحة تابعين للأمم المتحدة في عام 1996 و1997. وقد استخدموا مختلف الطرق للتجسس منها: التنصت على المكالمات، وزرع مخبرين وجواسيس في معسكرات الأمم المتحدة. وقد صرح وليام كوهين، وزير الدفاع الأمريكي، في مقابلة تلفزيونية: "لقد راقب العراقيون كل خطوة وكل حركة حاول أن يقوم بها المفتشون. وقد توقعوا الأماكن التي سيزورونها. بل يحتمل جداً أنهم استطاعوا اختراق فريق التفتيش ذاته". وقد صرح مسؤولون: "أنه يحتمل أن يكون فريق التفتيش ذاته تحت المراقبة في مقر الأمم المتحدة في نيويورك" (Weiner, 1997).

إن أكبر وكالة استخبارات في العراق وهي وكالة الاستخبارات العراقية، هي المسؤولة عن الاستخبارات والتجسس خارج البلاد، وما وراء البحار. ويعتقد أن هناك من يعمل خارج البلاد تحت ستار وظائف دبلوماسية. وتعمل هاتان الوكالتان تحت أمر منظمة الأمن الخاص والتي تجمع البيانات والمعلومات عن التهديدات الداخلية والخارجية ضد العراق". وفي19 تشرين أول/ أكتوبر عام 1997، قامت خدمات الأمن العام في إسرائيل (شبك) بإلقاء القبض على جاسوسين متهمين بالتجسس لصالح الاستخبارات العراقية العسكرية. أحد هذين المتهمين، وعمره (37) عاماً واسمه يوخار فران هاجر إلى إسرائيل بأوراق مزورة تعرِّفه بأنه ابن عائلة يهودية بقيت في العراق. وأما الشخص الآخر وعمره (30) ثلاثون عاماً وأيضاً حصل على جنسية إسرائيلية، وقد عمل كلاهما من مرفأ "أشدود" (Stutz&Glave, 1998).

4- التجسس الإلكتروني

كما أن الولايات المتحدة الأمريكية وحلفاءها كان لديهم مصادر تجسسهم الخاصة والتي اشتملت على صور من الأقمار الصناعية، وطائرات تجسس دون طيارين، والجنود الفارين العراقيين. وفي عام 1990 استطاعت الأقمار الصناعية الأمريكية للتجسس اكتشاف قوات عسكرية عراقية كبيرة على الحدود الكويتية، علماً بأنه تمَّ استبعاد احتمال غزو عراقي بعد أن صرح التحالف العربي بأن العراق إنما يتبجح فقط. وكذلك، فقبل أن تندلع الحرب، استطاعت نظم المسح للأقمار الصناعية رسم صور وخرائط لمناطق الأهداف المحتملة. ولقد وضعت هذه الخرائط على متن قاذفة الصواريخ توموهوك أثناء الحرب، وقورنت بالصور التي أخذت بواسطة رادار قاذفة الصواريخ ذاتها. ولقد ساعد نظام تحديد المواقع الكوني GPS، وهو نظام يتألف من مجموعة من (24) قمراً صناعياً تصدر إشارات تُسْتَخْدَم لتحديد الموقع، ساعد القوات الأرضية للحلفاء في التحرك الصحيح في التضاريس الصحراوية. ولقد استخدم نظام تحديد المواقع الكوني من قبل الطائرات لمسح الحقول الأساسية بمنتهى الدقة من قبل السفن الحربية الأمريكية للحصول على الإحداثيات الصحيحة لإطلاق الصواريخ. ولقد حلقت الطائرات بدون طيار ودارت فوق أرض المعركة مستخدمة جهاز تصوير فيديو وجهاز مسح إلكترونياً يعمل بالأشعة فوق الحمراء لتوفير بيانات تكتيكية قتالية حقيقية تبين تحركات الجنود العراقيين وتقديرات القصف. وقد قامت هذه الطائرات بطلعات بلغت (530) مهمة، وبمعدل (1700) ساعة طيران فعلية. بل إن بعض المقاتلين العراقيين استسلموا أمام واحدة من هذه الطائرات (Mazar, Snider, and Blackwell, 1993).

ولقد تمَّ تجهيز وكالة التجسس الإلكتروني العراقية المعروفة المشروع859 بأكثر من (1000) ألف فني ومحلل يراقبون المكالمات الهاتفية عبر الأقمار الصناعية وغيرها من ستة مواقع مراقبة وتنصت في الراشدية حيث يوجد مقر المشروع 859. ويتم هناك التنصت على الرسائل وتحليلها من قبل ضباط مخابرات عراقيين. ويحتمل أن يكون لدى هذه الوكالة القدرة على حل شيفرات بعض الرسائل المشفرة (Weiner, 1997).

وتراقب "العيون والآذان" الأمريكية العراق لتضمن التزام العراقيين بالاتفاقيات الملزمة بتفتيش الأسلحة. وأما نظام المراقبة الجوية فهو ذو ثلاث طبقات: (ثقب مفتاح الباب) المعروف باسم KH11 والنظام التصويري من الأقمار الصناعية التي تدور على

ارتفـاع تقـريبي قـدره (660) مـيـلاً. والقـوات الجـوية الأمـريكيـة U2Rمن طائرات التجسس الأمريكية التي تعمل من ارتفاعات تزيد على (90000) ألف قدم. والقوات البحرية " ES3A " (الظل) طيارة الفايكينغ، والتي تستطيع التقاط إشارات أجهزة الراديو العسكرية من ارتفاع (43000) قدم. وفي حزيران/ يونيو1998 عرض ريتشارد بتلر، الدبلوماسي الأسترالي الذي تمَّ تعيينه لمهمة خاصة من قبل الأمم المتحدة وهي نزع أسلحة الدمار الشامل العراقية، عرض صوراً تبين أنه يحتمل أن تكون العراق قد دفنت بعض قطع الصواريخ، ثم عادت لاستخراجها ثانية بعد التفتيش. وقد تمَّ عرض هذه الصور المدعومة بصور من الأقمار الصناعية كدليل على أن العراق لاتزال تخفي أسلحة غير قانونية.

وقد احتالت العراق عمداً لتخفي برامج أسلحتها. ففي أواخر عام 1997، وأثناء توقف مفتشي الأمم المتحدة عن البحث لمدة ثلاثة أسابيع عندما كانوا يبحثون عن الأسلحة المخفية نقلت العراق معدات يمكن استخدامها لإنتاج صواريخ ممنوعة خارجة عن مدى مراقبة آلات تصوير الأمم المتحدة. وادعى بتلر أن هذه المعدات تشتمل على معدات موازنة تدوير جيروسكوب والتي يمكن استخدامها لموازنة جيويكوبات الصواريخ المحظورة. كما قال أيضاً أنه يبدو أن العراقيين قد عبثوا بآلات تصوير الأمم المتحدة، وغطوا العدسات، وأطفأوا الأنوار في مواقع المراقبة. كما أنه تمَّ نقل أجهزة الكمبيوتر والأقراص الصلبة والمرنة التي تحتوي على معلومات هامة عن البرنامج النووي العراقي، والجرثومي البيولوجي والكيميائي، حيث كانت تنقل من مكان إلى آخر بشكل مستمر لإتعاب فريق تفتيش الأمم المتحدة.

وقد استمر العراق باستخدام الرسائل النفسية وإدارة التفكير. وعندما عاد مفتشو الأمم المتحدة لمتابعة أعمالهم بعد المشاكل التي منعت الأمريكان من أن يكونوا مع فريق التفتيش، فقد قام آلاف العراقيين بمظاهرات يندّدون فيها "فلتسقط أمريكا" عند مشاركتهم في تشييع عشرات الأطفال. وقد أوقعت العراق اللوم في موت الأطفال على مقاطعة الأمم المتحدة للعراق حيث إن الأطفال ماتوا بسبب نقص الغذاء والدواء (Associated Press, 1997).

5- زرع الفيروســات

تذكر إحدى الروايات أن قوات التحالف عطلت أيضاً نظم الكمبيوتر العراقية باستخدام "فيروس" تمَّ شحنه إلى العراق من خلال شحنة من "الطابعات". وقد تمت إذاعة هذه القصة في 1992/1/10 على قنوات شركة الإذاعة الأمريكية من خلال برنامج: "نايتلاين" (Nightline) بعد نشره في مجلة الأخبار الأمريكية والتقرير العالمي (U.S. News & World Report) الذي نص على ما يلي: وجهت الحكومة الأمريكية الفيروس إلى سلاح الدفاع الجوي العراقي. وقبل أسابيع من عملية عاصفة الصحراء، تمَّ شحن شريحة محملة بالفيروس قصداً، ووضعت في طابعة نقطية تمَّ تجميعها في فرنسا وتمَّ شحنها إلى العراق عن طريق عمان في الأردن. وادعى المصدر أنه تمَّ تطوير هذا الفيروس من قبل العاملين في وكالة الأمن الوطني (NSA) وتمّ تركيبه من قبل وكالة الاستخبارات المركزية الأمريكية (CIA). ويبدو أن هذا الفيروس كان قادراً على تعطيل كل من برامج وندوز وبرامج الكمبيوتر العملاقة أيضاً. وتدعي المصادر أن هذه العملية كانت ناجحة.

ولقد انطلقت هذه القصة من مجلة جون جانتس الأسبوعية (Gantzs Weekly Infoworld) حيث كتبت في أحد أعمدتها في 1 نيسان/ أبريل/ 1991 عن ذلك الخبر قائلة: "استطاعت وكالة الأمن الوطني كتابة برنامج فيروس باسم: ""AF/91" باستطاعته مهاجمة برنامج الطابعة والتحكم بالشاشة. وأضاف الخبر: وبحلول الثامن من كانون الثاني/ يناير/ 1991، أكدت قوى التحالف أن نصف الشاشات والطابعات كانت عاطلة عن العمل. واختتم المقال بما يلي: "وما رأيك بسرٍّ أخير؟ إن معنى " "AF/91 هو: "كذبة نيسان/ 91". ويعلق ون شوارتو: "إن " "AF/91 تعني "كذبة نيسان" 1991. وبناء على رسالة من جانتس إلى شوارتو، فقد أخذت مجلة "إنفو وورلد جابان" (عالم المعلومات اليابان) المقالة وترجمتها إلى اليابانية، وقد فقدت عبارة "كذبة نيسان" معناها أثناء عملية الترجمة. وقد تلقت مجلة "يو. إس. نيوز" (الأخبار الأمريكية) هذه المقالة من مكاتبها في طوكيو، والذي تلقاها بدوره من "انفو وورلد جابان". وهكذا، فقد بدأت هذه كنكتة أولاً، ثم أصبحت خبراً وطنياً. لقد كانت "كذبة"، وأي كذبة (Schwartau, 1994).

6- العلميات النفسية

أ ـ التلفزيون والمحطات الفضائية :

إن معرفة معتقدات الخصم عملية هامة في تصميم العلميات النفسية. فعندما أعلن العراق استخدام الغرب كدروع بشرية ووضعهم في الأماكن الحساسة، استثمر الغرب معرفته بالمعتقدات الإسلامية (العراقية) حيث ذكر القرآن أنك يمكن أن تفعل ماشئت بعدوك ولكن يجب أن لا تؤذي أسرته (زوجته، وأطفاله) وبالتالي فإن أفعال العراق في هذا السياق أفعال «جبانة» في أن يختبئوا خلف الأطفال والأبرياء ويتنكرون للشريعة الإسلامية، مما جعل استجابة العراق سريعة بأنهم «يحمونهم».

إن معرفة الثقافة الخاصة بالخصم أمر هام في نجاح العمليات النفسية وقد تكون رسالة نفسية ناجحة في ثقافة، وغير ناجحة في ثقافة أخرى مثل : إن تشبيه الرئيس الأمريكي للرئيس العراق بهتلر لم تكن موفقة (Just like Adolph Hitler)، فبالنسبة للأمريكان فإن هذا الوصف وصف «تحقير»، ولكن بالنسبة للعراقيين وللمسلمين عامة فإن هتلر من حاول إبادة اليهود، والعراقيون يكرهون اسرائيل، وقد هدد الرئيس العراقي بحرق نصف إسرائيل قبل اندلاع الحرب. هتلر طرد الإنجليز والفرنسيين الذين كانوا يستعمرون الشرق الأوسط، وبالتالي فإن المقارنة بين «صدام» و«هتلر» في الثقافة العراقية مقارنة «مدح» وليست مقارنة «تحقير». فصدام مثل هتلر يكرهه الإسرائيلين ويريد أن يبعد الغرب عن الشرق الأوسط.

كما أن خطاب الرئيس العراقي الموجه للشعب الأمريكي لم يكن موفقا، فقد اعتقد أن وسائل الإعلام حكومية تسير من قبل الرئيس بوش، وهذا غير وارد في الإعلام الأمريكي لأنه إعلام خاص، وثانياً طلب موافقة الرئيس الأمريكي على بث خطابه في الوقت الذي لم يكن بحاجة إلى هذه الموافقة، وثالثاً لم يتم اختيار رسالة مؤثرة في الشعب الأمريكي، بل كان خطاباً تقليدياً عربياً يبين حجج تاريخية لأن الأمريكان لا يعرفون مثل هذا التاريخ ولايهمهم أن يعرفوا، ولا يمثل نقطة إقناع بالنسبة لهم، والأهم من ذلك أن الخطاب قد بث في وقت متأخر من الليل حيث إن الأمريكان كانوا في سبات عميق ولا أحد يشاهد التلفزيون ساعة البث.

تعرف وزراة الدفاع الأمريكية العمليات النفسية على أنها : «عمليات مخططة تصاحب معلومات ومؤثرات منتقاة موجهة إلى مستمعين أجانب للتأثير على

مشاعرهم، ودوافعهم، وتبريراتهم المنطقية وبأقصى درجة لسلوكيات الحكومات الأجنبية، والمنظمات، والجماعات والأفراد. إن هدف العمليات النفسية هو إغواء (Induce)، أو تعزيز الاتجاهات الأجنبية والسلوكيات المحببة لأهداف المرسل (IWS - Psyops, 2001).

لقد كانت حرب الخليج حرب خيالات وصور مثلما كانت حرب تقنية ومعلومات. حرب بين صور صواريخ سكود وصور لصواريخ الباتريوت وهي تعترضها، إنها حرب «رصاصة تعترض رصاصة»، كما وصفها العسكريون. هذا بالإضافة إلى ما تحمله الحرب من صور وخيالات أخرى، فهل كانت صواريخ سكود العراقية تحمل رؤوساً نووية أو كيماوية ؟ لقد ساعدت الباتريوت إبعاد اسرائيل عن الحرب والمحافظة على ترابط التحالف الدولي ضد العراق. القليل من الدول العربية أيد حملة الصواريخ العراقية، والغالبية استنكر العدوان خاصة على السعودية. لقد خسر العراق الحوار من خلال الصور والخيالات التلفزيونية.

في إحدى الليالي كانت حرب الخليج قد بدأت، وكان أحد الضباط يراقب البث التلفزيوني (من بغداد) وهو في مركز السيطرة في وزارة الدفاع الأمريكية، وينظر إلى ساعته ويتشاور مع برج المراقبة الذين يخططون الهجمات...... ويعرف بلحظة تدمير برج الاتصالات المركزي العراقي ويقول «إذا كانت صواريخ الكروز (Cruise) قد أصابت أهدافها . . . فإن التقرير (البث) سينقطع بعد . . . (وبدأ العد بالثواني) . . . وقال الآن (Williams a, 1992). لقد انقطع بث كل من (ABC)، و(NBC) مباشرة(وهذا يعني تدمير برج الاتصالات العراقي)، أما ال (CNN) فقد استمر البث لديها ذلك أنها كانت قد استأجرت خط هاتف خاصاً مع الأردن وتم ربطها قبل الهجوم، أما ال(ABC)، و(NBC) فقد كانتا تبثان من خلال مركز الاتصالات العراقي.

ولمدة أكثر من اسبوعين فقد كانت الـ(CNN) هي المحطة الأمريكية الوحيدة التي تبث من العراق. لقد كان بثه مزيداً وكاملاً، ولقد أظهرت حرب الخليج أن أنواعاً من الحرب والدبلوماسية، قد بدأت في التشكل. لقد أدى البث التلفزيوني المباشر وغير المباشر إلى الضغط على الحكومات وتحريك الرأي العام باتجاهات مختلفة، ولقد أصبح الدخول إلى الجبهات ونقل مجرياتها يضع الكثير من الضغوط على الحكومات

وعلى متخذي القرارات السياسية. إن التغطية التلفزيونية في حرب الخليج قد عرفت بظاهرة حرب ال(CNN)، (Wood Ward, 1992) ويمكن وصف الحرب ضد الارهاب (القاعدة وطالبان) في أفغانستان بأنها حرب قناة الجزيرة .

وقد استغل الطرفان التلفزيون أثناء حرب الخليج لمصلحتهما وذلك للتأثير على الرأي العام. وبعد غزو الكويت بفترة وجيزة كذب الحرس الجمهوري العراقي أمام الكاميرا بأنهم يتراجعون، وذلك لوكالة أنباء تلفزيونية دولية. وفي الحقيقة، لم تنسحب القوات العراقية ولكنها كانت تعزز قواتها وقبضتها على الكويت. وكانت التقارير الواردة من وكالة (CNN)من مراسلها بيتر آرنيت (Pert Arnett) في بغداد محرفة نظراً للوقت الضيق المحدد لها على القمر الفضائي ليستطيع فيه تنسيق التقرير المصور الذي يعده، ونظراً للجهود الحثيثة التي يبذلها المهتمون العراقيون الذي عكفوا على استخدام وكالة (CNN)كوسيلة للدعاية والإعلام. وقد حصل المراقبون العراقيون على نتائج عالية، قبل إذاعة شريط فيديو التقرير المصور الذي قدمه العراقيون على شبكة (CNN)حياً على الهواء. واستطاع إعلاميو العراق الاتصال المباشر مع التلفزيون الأردني الصديق مما أدى إلى حدوث مظاهرات في الأردن ضد الولايات المتحدة الأمريكية وقوات التحالف. وأحدثت بعض الحملات الدعائية العراقية ردّ فعل عكسياً وذلك عندما أعلن العراق أن العراق ستكسب الحرب لأن الشعب على استعداد للتضحية بآلاف الجنود، بينما لا يستطيع الأمريكان تحمل خسارة مئات من الجنود. فأدرك الجنود والقوات العراقية أن العراق سيضحي بهم، وأنهم هم الضحية. وادعى عدد من المحللين أن هذا عزز رغبة القوات العراقية للهرب من ساحات المعارك والاستسلام (Lamb, 1996).

وقد قامت القوات الأمريكية بعدد من المناورات البرمائية على امتداد الشواطئ السعودية أمام شبكة (CNN) في محاولة لإيهام العراق بأن قوات التحالف تخطط لهجوم باستخدام القوات البرمائية لضرب القوات العراقية على الحدود الكويتية. وأفلحت هذه الخدعة حيث رابطت ألوية عراقية لحماية الشواطئ ضد إنزال قوات التحالف لقوات على الخليج (Kammer, 1997).

ولبيان أهمية البث التلفزيوني أيام الحرب، قال الرئيس الأمريكي بوش (الأب): «لقد تعلمت من الـCNN أكثر مما تعلمت من CIA . . . في أغلب حالات الأزمات الدولية فإننا ننقطع عن وزارة الخارجية وتقاريرها . . . هذه التقارير هامة . . ولكنها

لا تصل في الوقت اللازم لاتخاذ القرارات» (Fialka, 1992, p. 20) .

لقد ساهم التلفزيون في نجاح الحملة العسكرية ضد العراق وإبعاد اسرائيل عن المشاركة. إن صورة صواريخ الباتريوت وهي تعترض صواريخ سكود في الليل فوق تل أبيب قد ساعدت في إبعاد الحكومة الإسرائيلية من مهاجمة العراق، وحل التحالف الدولي في حرب الخليج ((Gilliams, 1992 (b)) .

ولم تترك ال(CNN) وقتاً لهضم المعلومات واستيعابها، بل على القادة أن يستجيبوا فوراً للمعلومات التي تقدمها في تقاريرها. ان صورة طيار واحد لطائرة أمريكية (هيلوكبتر) وهو يجر في شوارع مقاديشو قد أدى إعلان إدارة الرئيس الأمريكي كلينتون الانسحاب من الصومال.

وبينت إحدى روايات الأخبار الجنود العراقيين يسحبون الأطفال الكويتيين من الحاضنات، وكانت القصة مضخمة ومبالغاً فيها من قبل شركة علاقات عامة أمريكية تمَّ الاتفاق معها من قبل مؤسسة تدعمها الحكومة الكويتية. وكان الشاهد الفعلي الحقيقي لهذا المنظر المرعب هو بنت السفير الكويتي في الولايات المتحدة الأمريكية وعمرها (15) سنة. ولم يجد معد ومقدم برنامج 20/20 في وكالة ABC جون مارتن سوى تأييد ضئيل لصحة هذه الحادثة. إلا أنه كان وقع كبير لهذه الحادثة في أثناء الأحداث على صانعي السياسات في الولايات المتحدة الأمريكية. ويروى أن الرئيس جوج بوش ذكر مأساة الحاضنات والمعاناة الناجمة عنها (8) مرات خلال (44) يوماً أثناء محاوراته عن الحرب، كما ذكرها أيضاً (7) من أعضاء مجلس الشيوخ الأمريكيين أثناء محاوراتهم عن الحرب. وبالتالي، فقد نجح قرار المشاركة في الحرب بفارق (5) خمسة أصوات فقط (De Caro, 1996) .

وتمتاز الرسائل الموجهة عبر التلفزيون والبث الفضائي بأنها أكثر اقناعاً في الحالات التالية :

1- الرسالة من طرفين أكثر إقناعاً منها عندما تكون من طرف واحد.

2- اسلوب الرسالة يؤثر في قدرتها الإقناعية.

3- الرسائل الحية (فيديو) أكثر إقناعاً خاصة عندما يكون المرسل أكثر موثوقية والرسالة بسيطة.

4- الحالات أكثر إقناعاً من الإحصاء.

5- المرسل أكثر اقناعاً إذا كان يبدو آمناً (لطيفاً، صديقاً، عادلاً)، مؤهلاً (مدرباً، ذا خبرة، ذا معلومات) وديناميكياً (فعالاً، حركاً، حيوياً).

6- رسائل الأفلام، أو الفيديو أكثر فعالية في تعليم المعرفة المتعلقة بالخصائص.

7- ظهور العواطف (الخوف) أكثر اقناعاً خاصة إذا كانت العواطف مخيفة (Stech, 1994).

ب. الإذاعة

لقد استخدم الراديو بفعالية كوسيلة من وسائل الدعاية، فقد استخدمت اليابان إذاعة خاصة بها (Tokyo Rose) لبث الموسيقى والدعاية، والكلمات التي تحبط قوات التحالف. واستخدم الألمان ميلدرد جيلر (Mildred Gillar) المعروف بـ(Axis Sally)، ولقد استخدم الأمريكان الخداع والعمليات النفسية لإقناع الألمان بأن يوم الاجتياح لن يكون (D-Day) لنورمندي بل كاليس (Calais).

ومن الاستخدام المبدع للحرب النفسية في الراديو كان لإذاعة إل. بي. بي. سي (BBC) خلال شهر 1940/9م، عندما كان اجتياح الألمان لإنجلترا قد أصبح أمراً محتوماً، لقد بدأت ال بي. ي. سي. بث برامج تسمع بسهولة من الألمان تحت سلسلة من الدروس الإنجليزية للغزاة وقد بث هذا البرنامج بالألمانية.

لقد بدأ البرنامج على النحو التالي :

«. . . من الأفضل أن تتعلم بعض الكلمات والجمل القصيرة المفيدة في انجلترا مثل ان تزورنا. الدرس الأول. فإننا نأخذ الموت لعبور القناة».

والآن أعد بعدي: «القارب يغرق . . . القارب يغرق» «الماء بارد. . . الماء بارد».

والآن سأعطيك فعلاً مفيداً جداً، مرة أخرى / لطفاً أعد بعدي انني احترق، انت تحترق. انه يحترق. نحن نحترق. انت تحترق».

لقد استخدم الراديو في العمليات المعتمة (غير المعروفة) والعمليات النفسية بفاعلية في حرب الخليج، وقدر أن (87) ألف جندي عراقي قد استسلموا. لقد بثت إذاعة صوت الخليج الموجهة إلى الجيش العراقي رسائل تضمنت : الأخوة العربية، قوة التحالف الجوية، العزلة العراقية، وقد انتهت مهمة هذه الإذاعة بانتهاء الحرب.

ولقد استمرت الولايات المتحدة الأمريكية بعد الحرب استخدام الحرب النفسية من خلال وكالة الاستخبارات المركزية الأمريكية في محاولة للإطاحة بالرئيس العراقي. ولقد تمَّ القضاء على هذه العملية أخيراً من قبل الرئيس العراقي الذي استخدم الإذاعة ووسائل الإعلام الأخرى لإرسال رسائل مضادة. ففي مقابلة مع "وارن ماريك" عام 1997، وهو عميل وكالة الاستخبارات المركزية الأمريكية متقاعد، قال: "لقد أعدت شركة علاقات عامة ومركزها في واشنطن نصوص إعلانات إذاعية، وأشرطة فيديو تندد بالنظام العراقي. وقد استخدمت النصوص التي تطالب أفراد الجيش العراقي بالانسحاب والفرار تمت إذاعتها عبر محطتي إذاعة قويتين تابعتين لوكالة الاستخبارات المركزية الأمريكية تمَّ تأسيسهما وإدارتهما في جدة في المملكة العربية السعودية والكويت. بينما تمَّ إنشاء محطات إذاعة إضافية في كل من القاهرة وعمان. وقد أضاف "ماريك" أن طائرات بدون طيار قامت بإلقاء منشورات تسخر بالرئيس العراقي وتهزأ به في يوم مولده.

ج ـ الدعاية

إن استخدام الصور والخيالات (Images) والرموز الثقافية والخيالات والخرافات لتكوين ودعم عام وفعالية سياسية. فقد انتشرت أفلام الفيديو التي تمثل لقاءات الرئيس العراقي مع الوفود التي أمت بغداد حينها، وبيان حتمية النصر في المعركة. كما أن انتشار الإشاعات والعمليات النفسية من مثل أن الأفاعي في الصحراء قد هاجمت الأمريكان، أو أن صورة الرئيس العراقي قد شوهدت في القمر، ولم تنتشر هذه الإشاعات والتي مثلت أيام الأزمة الأولى معتقدات صفرية غير قابلة للنقاش ولا تخضع للمنطق ـ بين العامة من الناس وإنما بين المثقفين والأكاديميين.

ثم اتهمت العراق لاحقاً، الولايات المتحدة الأمريكية بأنها تخطط لضربات جوية لوضع مواد كيميائية مزيفة أو مواد جرثومية في "مواقع رئاسية" محظورة عن التفتيش، تستخدم كدليل ضد العراقيين. وقد أعلن بتلر وغيره عن شكوكهم بأن هذه المنشآت الضخمة، والتي يمتد بعضها عدة أميال تُسْتَخْدَم لإخفاء أسلحة الدمار الشامل عن المفتشين. وقدرت حكومة كلنتون أن هناك (78) موقعاً لهذه المواقع الرئاسية. وأن أحد هذه المواقع يغطي مساحة قدرها 31.5ميلاً مربعاً ويحتوي على 1058 مبنى.

وخلال هذه الفترة، أعلنت العراق على أنها "الفائز" في هذه المعركة عام 1998، وعرضت شاشات التلفزيون صدام متألق الوجه ملوحاً يده ببندقية قديمة يزور قرية بعد قرية. وكانوا المعجبون من الجماهير يرقصون ويصفقون ويغنون عندما يرون الرئيس يلوح بيده من الشرفة.

د. المنشورات الورقية

ألقت قوات التحالف أثناء الحرب (29) مليون نشرة بمختلف الأنواع خلف خطوط القتال العراقية. ووصلت هذه المنشورات إلى حوالي 98٪ من القوات التي بلغ تعدادها عندئذ حوالي (300000) مقاتل. وقد اختبرت هذه المنشورات على أسرى حرب متعاونين، الذين اقترحوا من ضمن توصياتهم إزالة أي أثر للون الأحمر (وهو علامة خطر للعراقيين)، وعرض القوات التحالف وقد أطلق أفرادها لحاهم (للتعبير عن الإخاء في مفهوم الثقافة العراقية)، وإضافة "الموز" (وهو فاكهة أثيرة ومفضلة) إلى طبق من الفواكه يقدم إلى الجنود العراقيين الذين يستسلمون. وقد تمت إذاعة "صوت الخليج" على ست موجات إذاعة، بما في ذلك محطات أرضية وهوائية. ولقد تمَّ بث ما مجموعه (189) رسالة عمليات نفسية خلال فترة تشغيل هذه الإذاعة أوائل عام 1991. كما تمَّت إذاعة رسائل أخرى من مكبرات الصوت محمولة، أو من العربات أو من طائرات الهيلوكبتر أثناء الحملات الأرضية (Lamb, 1996).

وقد ركزت المنشورات والرسائل الصوتية على حتمية هزيمة الجيش العراقي. وقد كان أكثر من (40%) من المنشورات يطالب القوات العراقية بالاستسلام، و(7%) تحث أفراد القوات العراقية على ترك أسلحتهم ومغادرة أرض المعركة. وقد كانت الرسائل التي كانت جزءاً من حملة رسائل العمليات النفسية والحرب النفسية تحاول طمأنة الجنود العراقيين بأنهم سيعاملون معاملة حسنة على يد قوات التحالف. وقد لامت هذه الرسائل النوايا الشيطانية لحرب العراق، وركزت على شجاعة المقاتلين العراقيين الذين ضللوا.

وأكدت الرسائل على الأخوة العربية والسلام أو حذرت القادة العراقيين من أنهم سيكونون مسؤولين وسيحاسبون على جرائم الحرب التي ارتكبوها ضد الشعب الكويتي وممتلكاته. ولمنع استخدام الأسلحة الكيماوية، حذرت هذه الرسائل الجنود العراقيين بأن تجهيزاتهم الوقائية ضد هذه الأسلحة هي رديئة، وأن القادة العراقيين سيعاقبون على ذلك (Lamb, 1996).

ووفق ما يدعيه الصليب الأحمر فإن حوالي (87000) جندي عراقي سلموا أنفسهم لقوات التحالف، وكان معظمهم يحمل تلك المنشورات أو يخفيها في ملابسه. ولقد بينت دراسة ميدانية بعد الحرب لعدد يبلغ (250) من أسرى الحرب أن (98٪) منهم قد رأوا هذه المنشورات، وأن (58٪) منهم قد سمعوا الإذاعة، وأن (34٪) منهم سمعوا مكبرات الصوت. واعتقد الجنود أن الرسائل الموجهة هي صادقة، وأن (88٪) منهم صدقوا ما جاء في المنشورات، وأن (46٪) منهم صدقوا إعلانات الإذاعة، و(81٪) منهم صدقوا ما يقال عبر مكبرات الصوت. وقد أكدت التقارير أن قرار أسرى الحرب بالاستسلام قد تأثر بتلك الرسائل، بينما قال (70٪) منهم بأنهم تأثروا بالمنشورات، و(34٪)منهم تأثروا بالإذاعة، و(16٪) تأثروا بما يقال عبر مكبرات الصوت. وقد أدلى لواء عراقي أسير بأنه: "في المرتبة الثانية بعد حملة القصف التي قامت بها قوات التحالف، كان لرسالة العمليات النفسية الأثر الأكبر على تهديد معنويات أفراد القوات العراقية" (Lamb, 1996).

ومن الأمثلة على المنشورات الورقية التي تم استخدامها ما يلي :

الطيران الإيراني في تزايد . . . لماذا؟

«لقد أعاد صدام الساحل لإيران، والآن يعطيهم قواتكم الجوية، هناك طريق مثالي للاختبار. اهرب إلى العربية السعودية. اتصل بنا بالراديو، وأعلن انضمامك لاخوتك العرب. تقدم وحدك في طائرتك . اخفض جير الهبوط، اشعل إضاءة الهبوط، جرد طائرتك من السلاح، وطر على سرعة لا تزيد على (250-300) عقدة، وبعد الانتهاء من هذه الأزمة سيسمح لك بالعودة لبلدك لإعادة بنائه».

وهذا المنشور موجه إلى الطياريين بالفرار إلى السعودية بدل أن تأخذ إيران (عدوهم لمدة 12 سنة) طائراتهم.

الاستسلام الآمن :

- أمام العسكر خياران: اما القتال أو الموت المؤكد.
- أو الاستسلام والحياة ورؤية أسرهم مرة أخرى.

الاستسلام الآمن

ـ افرغ البندقية من العتاد (من مخزن الذخيرة).

ـ انكس البندقية وضعها في كتفك الأيسر.

ـ ضع كلا يديك فوق رأسك.

ـ تقدم إلى القوة متعددة الجنسيات ببطء.

ـ إذا قمت بذلك تنجو من الموت.

– هذا هو الانذار الأخير

– سوف نقوم بقصف وحدتك غداً.

– اهرب من هذا الموقع حالاً.

المنشور التالي يبين رسالة موجه إلى معدات محددة ال(16 ,20 ,18) وإعلامهم أن قوات التحالف تيسيطر على الأجواء ويمكنها أن تغير عليهم في الوقت الذي تختاره، وأنهم غير قادرين على أي شيء لمنعهم، وهذا هدم للمعنويات. وعندما يسقط هذا المنشور على شكل قنبلة والتي عرفت باسم (Daisy Cutter) مع عبارة أنها أكثر قنبلة تقليدية تدميرية حربية لها قوة أكثر من (20) صاروخ من صواريخ سكود.

«أهربوا وحافظوا على حياتكم، أو أبقوا وواجهوا الموت».

وعلى الخلف عبارات: «لقد عانيتم الكثير من الخسائر لأننا استخدمنا أكثر الأسلحة فتكاً وقوة في هذه الحرب، إنها أقوى من (20) صاروخ من صواريخ اسكود نحذركم، سندمر موقعكم ثانية ... الكويت ستحرر من عدوان صدام أسرع والتحق باخوتك من الجنود .. سنعاملك بكل الاحترام والحب. أهرب من هذا الموقع لن تكون أبداً سالماً».

وقد كان برنامج العمليات النفسية، أو الحرب النفسية العراقية أقل نجاحاً من الحرب النفسية لقوات التحالف، وكان أحد أسباب فشل الحرب النفسية العراقية أن العراقيين لا يفهمون الثقافة الأمريكية. فعلى سبيل المثال، فقد استخدموا امرأة تدعى: "بغداد بيتي" لإعداد مادة إذاعية تهدف إلى تضليل الجنود الأمريكيين. ولقد فقدت مصداقيتها قبل ذلك عندما أعلنت لهم أن زوجاتهم وصديقاتهم سيضاجعن كلاً من:

توم كروز، وتوم سيليك، وبارت سيمبسون" . وكان من الغباء بمكان أن تقترح المذيعة أن نساء الجنود الأمريكيين سيغويهن أبطال السينما والأفلام، وليس شخصيات أفلام الكرتون.

بحثت جماعة العمليات النفسية الرابعة (Airborne) وطورت أكثر من (29) مليون نسخة من (38) منشور مختلف (حوالي 29 طن). تضمنت المواضيع التالية:

الاستسلام، تفوق قوات التحالف والأمريكية، الحتمية، صدام هو السبب، الإخلاء، والهروب،وكان توزيعهم هذه المنشورات وفق مواضيعها على النحو التالي:

جدول رقم (14)

موضوع المنشورات وحجمها التي ألقيت على العراق

موضوع المنشور	الإجمالي
الاستسلام	12.4 طن
الحتمية	6.6 طن
الإخلاء والهروب	1.9 طن
خطأ صدام	4.7 طن
أخرى	3.5 طن
المجموع	29.1 طن

المصدر : http://www.pipeline.com/-psywarrior/gulf1.html. p.1

وفي نهاية الحرب، صرح اللواء الروسي إس. بوغدانوف، رئيس الأركان لمركز العمليات والشؤون الاستراتيجية قائلاً: "لقد خسرت العراق الحرب قبل أن تبدأ. لقد كانت هذه الحرب حرب تجسس، وحرباً إلكترونية، وأوامر وسيطرة وعمليات تجسس. لقد أعمي أفراد القوات العراقية وأصموا. ويمكن كسب الحرب الحديثة باستخدام المعلومات، وهي الآن أمر حيوي وهام تماماً" . ولقد لعبت الحرب النفسية أيضاً دوراً هاماً ليس مع الجنود العراقيين فحسب، ولكن مع الرأي العام أيضاً. فعندما تمَّ تحرير مدينة الكويت، عرضت وكالات الأنباء المتلفزة مئات الأفراد الكويتيين

يلوحـون بالأعـلام الأمريكيـة على أنهـا هي قـوات التحـرير التي دخلت المدينة وتبين تأييدها للقوات الأمريكية. وقد رتبت شركة للعلاقات العامة في وقت مسبق توزيع كميات كبيرة من الأعلام الأمريكية وغيرها من وسائل الدعاية (Rendon, 1996).

هـ . الخداع (Deception)

عمليات الخداع والعمليات السرية عمليات معقدة وتتطلب ذكاء وأساليب ومصادر، ومن أمثلة هذه العمليات ما قام به الحلفاء لاقناع هتلر وقيادته أن قواتهم ستغزو أوروبا من خلال شواطئ قريبة من باسي دي كالاس (Pas de Calais) وليس من نورمندي (Normandy) والتي تبعد حوالي (100) مائة ميل. مما جعل الإلمان يعتقدون أن «جماعة باتون العسكرية» وهي غير واقعية هي القوة المعدة لهذا الهجوم من خلال القنال الانجليزي والتي تحميها القوات الألمانية (Isth Panzer). اعتقد الألمان بحقيقة الخدعة وأن الحلفاء سيهاجمون من خلال كالاس تحت قيادة الجنرال جورج سي. باتون (Patton) ونتيجة لذلك وضعوا أفضل قواتهم في فرنسا في كالاس ينتظرون باتون. وحتى عندما وصل غزو الحلفاء إلى نورماندي لم يسمح هتلر بنقل قواته (Isth Panzer) من كالاس لأنه كان معتقداً أنه فقط مقدمة للغزو الحقيقي. ولقد بقيت قواته تنتظر حوالي (7) أسابيع للغزو الذي لم يحدث أصلاً (Rue, 1994).

و ـ الخطابات (Speeches)

إن بقاء الاتحاد السوفياتي خلال الحرب العالمية الثانية قد عُزي إلى قدرة ستالين لاستعادة وتحريك مشاعر الروس. لقد تنبه ستالين إلى أن الإيدولوجيا المجردة والشعارات الشيوعية التي كونها الحزب في عقول المواطنين منذ عام 1918م، غير فاعلة وليس لها تأثير عاطفي أو روحي لحفز الروس في صراعهم مع الجيوش الألمانية. ولذا تحول ستالين إلى تحديد النظام الشيوعي «روسيا المقدسة» و«وروسيا الأم» بحضارتها القديمة، ورموزها المصاحبة ولقد كان أعمق مؤسستين في هذا التاريخ هما الجيش والكنسية حيث حصدا دعاية ستالين كما لم يحصل من قبل في تاريخ روسيا، ولقد كانت إنجازات الجيش الروسي كبيرة، وعاد للظهور صحف مثل برافدا (Briavad)، واسقطت شعارها «عمال العالم والوحدة» وحل محلها الشعار الوطني «الموت للغزاة الألمان».

لقد وصفت كورتيا كنج (Coretta King) خطاب زوجها مارتن لوثر كنج عندما قال «لدي حلم» (I have a Dream) في عام 1963 تاركاً خطابه المكتوب، ناسياً الوقت، لقد تحدث من قلبه وانشر صوته بين الجمهور ليخبر العالم أجمع.

ومع تزايد التهديدات الامريكية لضرب العراق في عام 2002 يلاحظ تركيز خطابات وتصريحات الرئيس الأمريكي (بوش) على العدالة والحرية، وأسلحة الدمار الشامل، وخطورة الرئيس العراقي وتهديده لجيرانه وشعبه باستخدام أسلحة الدمار الشامل كل هذه المفردات للحصول على دعم الرأي العام الأمريكي لصالح الحرب ضد العراق.

7- الرقابة الإعلامية (Censorship)

إن أول ضحايا الحرب "الحقيقية"، الحقيقة لا تغتال فقط وقت الحرب، ولكنها في الغالب تفقد أو تحبس. وفي حرب الخليج حرص التحالف على أن تقوم وسائل الإعلام بتقديم الحقيقة كما يراها الجيش. وهذا الهدف تطلب خبطاً كبيراً لما تشاهده وسائل الإعلام وكيف تقدمه (تبثه). لقد حدد الجيش الوصول إلى ما يحدث في الميدان وإلى العمليات هناك، مما أتاح للجيش أن يربح تغطية إيجابية خلال الحرب على حساب عدم رضا المؤسسات الإعلامية، والشكوك حول إذا ما كانت تراه وسائل الإعلام يمثل الأحداث كلها (القصة الكاملة) (Williams, 1992a).

أـ **الانتقاء الإعلامي** (Pool Reporting): من خلال الانتقاء الإعلامي يمارس الجيش تحكمه في الإعلام، حيث يقوم الجيش بانتقاء من يقوم بالتغطية الإعلامية وتتم مشاركة وسائل الإعلام الأخرى له، مما تحصل علية تلك الوسيلة المنتقاة. تستخدم هذه الطريقة لأن مسرح العمليات لا يحتمل وجود العديد من الصحفيين.

خلال الحرب العالمية الثانية سمح لعدد محدود من الصحافيين بمرافقة الجيوش لتغطية عملياتها، وكان ذلك ناجماً عن كلفة إرسال الصحافيين إلى جبهات القتال. فمثلاً كان هناك (461) من المراسلين الصحفيين سمح إلى (27) منهم فقط بمرافقة الجيش إلى نورمندي في (D-Day)، (Ramsey, 1994).

وفي فيتنام كان الحد المسموح به في أي وقت (47) مراسلاً صحفياً، وكان هذا من أصل (400) صحفي، وهذا العدد القليل من الصحفيين بسبب طبيعة الحرب

الفيتنامية. وفي عملية جريناندا (Grenada) فقد مثلت انخفاضاً كبيراً في العلاقات بين الإعلام والجيش، فلم يسمح للصحافيين، أو المراسلين بدخول الجزيرة مع الجيش عدة أيام بعد بداية العملية (Benjamin, 1995).

وفي حرب الخليج كان هناك (1600) صفحي ومراسل صحفي في السعودية، خصص منهم (400) مع الوحدات المقاتلة في الحرب البرية، وهذا العدد من الصحفيين الكبير يشكل خطورة بالإضافة إلى وجود صحفيين أجانب في السعودية التي لم يكن فيها صحفيون أجانب قبل غزو الكويت. أما بقية الـ(1200) صحفي الذين لم يشاركوا في التغطية، فلم يكن الإعلام بحاجة إلى وضع محظورات.

لقد وضعت قوات التحالف الشروط التالية على الصحفيين الذين يعملون من السعودية وعدم الالتزام بهذه الشروط يعرض الشخص إلى الترحيل، والشروط هي:

1- عدم ذكر عدد محدد من الجنود، أو الطائرات، أو المعدات ... إلخ، فقط عبارات عامة لوصف القوة المتوافرة.

2- عدم ذكر أي خطط مستقبلية.

3- عدم ذكر مكان الوحدات العسكرية.

4- عدم ذكر طرق استخدام القوات المتحالفة للقوة.

5- عدم ذكر المعلومات الاستخبارية المجمعة.

6= عدم ذكر تحركات القوات العربية طالما أن هناك التحاماً عسكرياً.

7= عدم ذكر مكان إقلاع الطائرات.

8= عدم ذكر معلومات عن فعاليات أو عدم فعاليات قوات الخصم.

9- عدم ذكر معلومات عن الطائرات المسقطة أو السفن أثناء البحث عن المفقودين.

10- عدم ذكر طرق قوة العمليات أو المعدات الفريدة.

11- عدم ذكر طرق التشغيل والتكتيكات بصفة عامة.

12- عدم ذكر الانكشافات في العمليات والدعم إلا بعد أظهار المعلومات من القائد العام.

والمتطلب العام هو البقاء برفقة العلاقات العامة في القواعد السعودية وحق التصرف(Discretion) للقائد (Commander) في القواعد الأمريكية. جميع تقارير المراسلين الصحفيين ترسل إلى مكتب المعلومات المشترك و إلى الظهران، والمكان الرسمي للمراقبة الخاص بالمراجعة الأمنية.

قسمت التغطية الإعلامية في حرب الخليج إلى أربعة أنواع هي: المطبوعات، والتصوير، والراديو، والتلفزيون، وكل هذه كانت ذات إطلاع محدود جداً على مجريات الحرب

ب- المراقبة الإعلامية بالتأخير: من أكثر الشكاوي خلال عاصفة الصحراء هو تأخيرالتقارير الواردة من الجبهة، ففي أفضل الأحوال كانت مقطوعة الفيديو يستغرق نشرها من لحظة قدومها من الجبهة يوم كامل، وبالمعدل تستغرق (٣) أيام. ومن أسباب التأخير هو المسافة الكبيرة داخل مسرح العمليات وأخذ التقرير إلى الدمام من مؤسسة (Vii Corps) يتطلب السفر مسافة طويلة حتى مدينة الملك خالد العسكرية (KKMC) حيث ترسل التقارير منها إلى مدينة الدمام، والسبب الثاني هو الأولوية الدنيا التي أعطاها الجيش للإعلام. وكان الأصل أن ترسل التقارير بسيارة عسكرية وبعد الاحتجاج من المراسلين تم استخدام طائرة هيلوكبتر (Benjamin, 1995) والخلاصة أن تأثير الإعلام في حرب الخليج كان ضعيفاً، وقد كان الإعلام بعيداً عن مركز الفعاليات عمداً وأحياناً دون قصد من قبل الجيش الذي لازال يتذكر فيتنام. وأن المعلومات ليست حرة في زمن الحرب، ان نشر المعلومات أو بثها في الوقت الخطأ قد يؤدى إلى قتل الناس. الحجب ضروري وفي حرب الخليج تم حجب المعلومات.

ج- التنصت : تم رصد مكالمات الرئيس العراقي صدام من خلال التغلغل في «انسكوم» ودون علم بتلر، حيث تبين أنه يستخدم المساعدين لإجراء المكالمات بواسطة أجهزة هاتف آمنة منتشرة في جميع أنحاء بغداد، بالإضافة إلى جهاز هاتف مثبت في سيارته ويعمل بالراديو. ويذكر هييرش الكاتب في صحيفة نيويورك أنه في مطلع عام (1998) أمكن فك الشيفرة وأصبحت مكالمات الرئيس صدام مكشوفة للجنة انسكوم «ولقد قمت بدراسة هذه المكالمات للتنبؤ بشخصيته وذلك للتأثير عليه والتحكم في سلوكه وذلك لأنه الشخص الذي يصدر القرارات العسكرية ويبني السياسات (الخليفة، 2000م).

الجزء الثالث:

حرب المعلومات الهجومية

- ☐ الفصل السابع: المصادر المفتوحة.
- ☐ الفصل الثامن : العمليات النفسية وادارة النفس والادراك
- ☐ الفصل التاسع : الداخليون
- ☐ الفصل العاشر : مصادرة الاشارات
- ☐ الفصل الحادي عشر: الاختراق
- ☐ الفصل الثاني عشر: التنكر والخفاء
- ☐ الفصل الثالث عشر: الوباء الفضائي

تمهيد

يتناول هذا الجزء أساليب حرب المعلومات الهجومية، وهي أساليب متنوعة يمكن القيام بها من قبل أفراد عاديين أومن قبل أفراد محترفين. ويمكن وصف هذه الأساليب بأنها تشكل أسلحة فوضى شاملة (Mass disruption) في البنية التحتية المعلوماتية في أي مجتمع، ويتناول هذا الجزء أهم أساليب حرب المعلومات الهجومية، والموجهة إلى البناء التحتي المعلوماتي للمجتمع ولمصادر المعلومات فيه. وتشمل هذه الأساليب: والمصادر المفتوحة، والعمليات النفسية، والداخليين من المنظمة ذاتها، والاعتراض المعلوماتي، والاختراق والتنكر والخفاء، والأوبئة المعلوماتية.

يتناول الفصل السابع المصادر المتاحة أو المفتوحة وكيفية استغلال المعلومات المتوافرة فيها لشن عمليات تخريب وعدوان على الطرف الآخر (العدو). اما الفصل الثامن فيتناول العمليات النفسية وإدارة النفس أو الإدراك النفسي، وكيفية التأثير على عقل العدو وتوجيه سلوكياته ومعتقداته بالاتجاه الذي يسهل عملية الفوز والنصر عليه ويضعف من معنوياته. كما يتناول الفصل التاسع الداخليين من خلال زرع الجواسيس والخونة ونشر الفساد عامة بين صفوف العدو وذلك بأساليب الإغراء المادي والمعنوي للأطراف المتعاونة في هذا المجال. أما الفصل العاشر فيتناول الاعتراض الفضائي وتحويل مسار المعلومات بالاتجاه الذي يمكن من الاستفادة منها واستغلالها أو تدميرها، أو تحريفها، في حين يتناول الفصل الحادي عشر الاختراق، ويشمل الدخول غير المشروع . ويتناول الفصل الثاني عشر التنكر والخفاء مثل سرقة الهويات وأسماء الدخول، وكلمات السر، ويتناول الفصل الثالث عشر الأوبئة المعلوماتية مثل الفيروسات كأدوات عدوان وتخريب وما تسببه من خسارة معلوماتية كبيرة .

الفصل السابع

المصادر المفتوحة

مقدمة

يقصد بالمصادر المفتوحة (المصادر العامة أو المتاحة) المصادر المعلوماتية المتاحة لعامة الناس كالصحف، والمجلات العلمية، والنشرات، والتقارير، والنشرات الحكومية، والانترنت، والكتب . . . إلخ.، وتُعد هذه المصادر مصادر لاكتساب المعلومات، وتشمل بشكل محدد المصادر المفتوحة (المتاحة)، والاستخبارات التنافسية وخرق (التعدي) الخصوصية.

ويعد الحصول على المعلومات من خلال المصادر المفتوحة أمراً سهلاً، ولا يشكل في أغلب الحالات خرقاً للقانون أو الخصوصية، حيث أن هذه المعلومات متاحة للجميع. وتتمثل خطورة المعلومات المجمّعة من خلال المصادر المتاحة عند موالفتها مع بعضها البعض بحيث تكون وحدة واحدة متكاملة في موضوع ما، خاصة إذا كان هذا الموضوع يتعلق بالتقنيات العسكرية أو الاقتصادية أو الأسرار الاقتصادية أو العسكرية . . . الخ. ومع توافر الانترنت بشكل واسع في العالم، فإن الوصول للمعلومات من خلال الانترنت قد أصبح من السهولة بمكان وعلى نطاق واسع. لا بل أن الانترنت أكبر مصدر معلومات مفتوح على مستوى العالم، وتمتاز بأن أي فرد من أي مجتمع يمكنه الوصول اليها ومن أي مكان. وفيما يلي استعراض لأهم المصادر المفتوحة في جمع المعلومات.

المصادر المفتوحة

1- استخبارات المصادر المفتوحة

يعني مصطلح استخبارات المصادر المفتوحة (Open Source Intelligence [OSINT]) عمليات الاستخبارات التي تستخدم المصادر المفتوحة من المصادر غير المحظورة، ومثلها مثل بقية الأنواع من الاستخبارات، فإنها لا تتوقف عند جمع المعلومات. إنها تشمل تحليل المتطلبات، تصفية المعلومات وتحليلها، وتكاملها بعد جمعها. إن الهدف من هذا النوع من المعلومات المساعدة في الحصول على إجابات مهمة لهدف ما، أما الاستخبارات المتنافسة (Competitive Intelligence) فتعني الاستخدام المؤسسي لاستخبارات المصادر المفتوحة ضد منافسين في الأعمال. وقد يتم

جمع معلومات حساسة من مصادر متعددة غير محظورة ويتم دمجها لتشكل وحدة متكاملة، أو قد يتم استنساخ معلومات هامة من المعلومات المجمعة من المصادر العامة.

إن استخبارات المصادر المفتوحة رخيصة، ويمكن الحصول عليها بسرعة وسهولة، ولا تحتاج لوقت كبير في جمعها، وهي قانونية إلا إذا خرقت الخصوصية وحقوق الإنسان، وحقوق الملكية، وهي غير خطرة على العملاء. ومن الأمثلة الحديثة على ذلك (العميل الأمريكي الذي سجن في روسيا وأُفرج عنه بقرار من الرئيس الروسي بوتن) والذي اتهم بالتجسس لصالح الولايات المتحدة، حيث أكد الدفاع عنه بأنه حصل على المعلومات من المصادر المفتوحة، وهي قانونية ومتوافرة للجميع ولم يقم بخرق حقوق الآخرين . . . أو فعل مخالف للقانون.

ويرى جورج كينان (George Keenan) أن (95%) من ما ترغب الحكومة الأمريكية معرفته يمكن الحصول عليه من الدراسة الدقيقة للمعلومات المفتوحة والمتوافرة في المكتبات، والأراشيف المتوافرة في البلاد. أما غالبية الباقي فيمكن الحصول عليه من مصادر مشابهة في الخارج (Keenan, 1997).

2ـ المتصفحات (Browsers):

هي برامج التصفح على الإنترنت ومن أشهرها نتسكيب (Netscape) واكسبلورير (Explorer). وهناك ثغرات في المتصفحات تجعل الدخلاء يتمكنون من الوصول إلى حاسبك ومعلوماتك الشخصية بينما أنت تتصفح في الشبكة. هذا بالإضافة إلى المعلومات المدونة على الشبكة عن أي شخص مثل دليل الهاتف، السجلات الحكومية، والمدارس، والجامعات، ومكان العمل، والإعلام . . . إلخ.

3ـ بروتوكول النص الفائق (HTTP).

يُمكن بروتوكول النص الفائق مواقع الإنترنت والمتصفح من الاتصال وتبادل الوثائق والصور والصوت. والمصطلح الفني لموقع صفحة ما هو ما يعرف (Uniform Resource Location [URL])، فمثلاً .http://www.privacy.gov. au هو الـ(URL) لهذه الصفحة. وهناك بعض الجوانب في بروتوكول النص الفائق تجعل من الممكن تتبع نشاطاتك، ويمكن زيارة موقع (http://www.uiuc.edu/cgi-bin/inro) لمعرفة المعلومات التي يرسلها متصفحك على كل صفحة طلبتها.

4ـ تحميل البرمجيات المجانية (Downloading):

هناك مئات المواقع التي تقدم برمجيات مجانية يمكن تحميلها من الإنترنت، وقد تتطلب بعض المعلومات عنك أو قد ترسل بعضها دون علمك، وغالبية هذه المواقع لطلب ملء استبانة الكترونية تتضمن معلومات عنك مثل الاسم والعنوان البريدي واهتماماتك. . . الخ.

5- محركات البحث (Search Engines):

هي أدوات على الشبكة تُمكن من البحث عن المعلومات، وهي كثيرة أهمها (Yahoo, Altavista, Google, Hotbot) وبعضها يوفر خاصية البحث عن الأفراد ومن الممكن أن تبحث تحت مواقع البرامج المجانية، وتكشف معلومات عنك.

6-البريد الإلكتروني (E-mail):

يُمكن للبريد الإلكتروني أن يهدد خصوصية الفرد حيث يشمل على اسم الشخص، أو ما يستخدمه للدلالة على اسمه، وهو ما يسبق @ أما ما يتبع الـ @ فهو خادم الإنترنت أو ما يسمى (ISP) أو اسم المنظمة التي يعمل فيها الفرد @Mutah حيث (Mutah) جامعة مؤتة، ومايتبع ذلك نوع القطاع أما ما يسمى (Domain) وهو (Edu) أي قطاع تعليمي، وأخيراً اسم البلد مثل (Jo) وذلك للدلالة على الأردن وبالتالي يمكن تحديد العنوان البريدي (Badayneh@Mutah.edu.jo) على أنه البداينة @ جامعة مؤتة. قطاع التعليم. الأردن. وبالتالي يمكن الوصول للشخص أو أخذ معلومات إضافية من الأصدقاء أو العاملين.

ويمكن اعتراض بريدك الإلكتروني (مثل أي شخص يمكن أن يعترض بريدك الورقي العادي). ويمكن استخدام برامج تشفير مثل (Pretty Good Privacy [PGP]) وهو برنامج مجاني لحماية المعلومات المرسلة بالبريد. هناك مئات برامج جمع العناوين الالكترونية التي تقدم بجمع جميع العناوين على خادم معين مثل: mutah. Edu. Jo ومن أمثلة هذه البرامج برنامج (direct E-mail Collector).

7- بريد القمامة (Spam):

هناك بعض المواقع التي تسعى للحصول على عناوين البريد الإلكتروني للآخرين لكي تمطرهم بالدعايات التجارية. فيمكن الحصول على هذه العناوين من خلال

الاشتراك في جماعات النقاش أو الأخبار . . . إلخ.، ولدى مثل هؤلاء الأفراد برامج لتكوين قائمة عناوين وفق الاهتمامات وإمطارها بالدعايات. والمشكلة هي في قراءة هذه الدعاية ومحوها من البريد لأن ذلك يستغرق وقتاً، وفيه هدر للوقت والجهد الذي يبذله الناس في محو هذه الدعايات (APCW, 2001). كما يمكن استخدام برامج جمع العناوين البريدية لهذه الغاية. وتقوم الشركات حالياً بجمع العناوين من على خادمات الانترنت وارسال دعاياتها إليها.

8- التجارة على الإنترنت (Internet Commerce):

يزداد استخدام الانترنت يوم بعد يوم كمكان للتسوق حيث يتوقع، أن يصل عدد المستخدمين في عام (2003) إلى (502) مليون مستخدم ومن المتوقع أن تصل التجارة الالكترونية في العام ذاته الى(1) ترليون دولار*.

إذا تعامل الفرد مع المواقع على الشبكة لشراء بعض ما يحتاج إليه، فقد يستخدم بطاقة الائتمان من خلال الإنترنت. الكثير من الناس يتسوقون بهذه الطريقة وبعضهم الآخر يعتقد بأن العملية غير آمنة. وبعض المواقع تطلب معلومات عن الفرد وقد تبيع هذه المعلومات إلى آخرين أو إلى المسوقين، ومن خلال المعلومات التي تحملها البطاقة(الرقم والاسم) ويمكن أن تستغل هذه المعلومات.

9ـ التفتيش في القمامة

يشير هذا إلى عمل البحث والتفتيش في القمامة عن الوثائق المرمية، والمواد المطلوبة. ومن الناحية القانونية هذا العمل مسموح ـ ولكن هذا غير مباح من الناحية الأخلاقية، ويقوم لصوص بطاقات الائتمان على تفتيش القمامات، وذلك بغرض الحصول على المعلومات الخاصة ببطاقات الائتمان من خلال الايصالات المرمية فيها ـ ويقول وينكلز (Winkler) بأن الجيش الأمريكي قد حدد لها وحدة تكرس العمل فيها للبحث عن القمامات. ولقد قام زعماء فرنسا من سرقة القمامة في هوستن لغرض الحصول على الأسرار الصناعية منها.

---

* Report to the president's working group on unlawful couduct on the internet.

ومن الأمثلة على ذلك سوزان تندر (Susan Thunder) وهي من لوس انجلوس كانت تلبس الملابس الرثة، وتمتهن نفسها مثل امرأة مشردة، ومشوهة عندما كانت تفتش في القمامة. بالاضافة إلى ذلك يستخدم البحث في القمامة للحصول على معلومات شخصية لبيعها والحصول على مبالغ طائلة من ورائها، حيث يقول بنجامين بيل (Baniamin Bell) بأنه قد قام بجمع (75) حقيبة من الأوراق التي تتضمن بيانات مصرفية، أي المراسلات القانونية والرسمية.

10- الشمشمة (Snooping):

وفي عام 1995، ظهر الدخول إلى عدد من الحاسبات في عدد من الولايات المتحدة الأمريكية، والمكسيك من جامعة هارفرد، حيث قام الدخلاء بترك أرقام هوياتهم (IDS)، ومعلومات عن كلمات السر على الحاسبات في تلك الجامعة. ولقد زاد اهتمام الولايات المتحدة الأمريكية عندما تبين أن الدخول قد وصل إلى الشبكة المدارة من قبل البحرية الأمريكية، والمعروفة باسم (NCCOSC)، حيث وصل الدخلاء إليها ووضعوا برامج الشم (Sniffer) لالتقاط الأرقام (IDS)، وكلمات السر الخاصة بالمستخدمين الرسميين ووضعوا برمجيات أخرى تمكنهم من الوصول للبيانات وتدميرها أو الحرمان من استخدامها.

وبعد مهاجمة أحد المواقع في تايوان، فقد تم تعقب الدخيل من خلال الدردشة على الإنترنت مستخدما اسم جريتون (Girton) وتم تعقبه إلى الأرجنتين، حيث تبين أنه معروف لدى السلطات الأرجنتينية كقرصان حاسب متخصص في الدخول غير الشرعي والتسلل وسرقة المكالمات الهاتفية والدخول لنظم الهاتف ويدعي جوليوسيسار أرديتا (Julio Cesar Ardita) وعمره (21) سنة، طالب في جامعة الأرجنتين. أما المواقع الضحية فكانت (62) موقعاً حكومياً أميريكياً، و(136) موقعاً تعليمياً، و(31) موقعاً تجارياً. ولقد اعترف بمسؤليته، وتمت مصادرة حاسبه. ولم تكن جرائم الحاسب من الجرائم المشمولة في تبادل المجرمين. وفي عام 1997م، وافق ارادياً على القدوم متطوعاً إلى الولايات المتحدة والاعتراف بذنبه بالدخول غير القانوني إلى حاسبات عسكرية وتدمير ملفات عسكرية ونظراً لتطوعة في القدوم حكم (3) سنوات وغرامة (5000) دولار (The Washington Post, 1996).

يمكن لكل فرد من أفراد المجتمع أن يقوم بجمع معلومات خاصة تتعلق بفرد آخر، وذلك عن طريق أصدقائه، أو عن طريق أعدائه، أو عن طريق شخص، أو أشخاص آخرين، كما يمكن جمع هذه المعلومات عن طريق برامج بسيطة تمكن من جمع المعلومات المطلوبة. ولقد تم تطوير نظام أثار ردود فعل سلبية من جماعات حماية الخصوصية، هذا النظام يسمى المفترس (Carnivore)، ويستخدم لتحليل الرسائل الإلكترونية بحثاً عن معلومات يتم تبادلها بين المجرمين، وهو قادر على تحليل الرسائل الصادرة، والواردة من مقدم خدمة معينة، ويمكن وضعه في مقدم خدمة الإنترنت وشركات الهاتف (US Today, 2001).

11- تصفح الوب (Web Browsing)

إن مشغلات المواقع على الوب يمكن أن تجمع معلومات عن الزوار لمواقعها . . . وخاصة عنوان (IP) لحاسب المستخدم، ونوع النظام، ونوع المتصفح، وعدد الصفحات، والوقت. . . إلخ. كذلك فإن غالبية المواقع تتطلب اسماً ومعلومات عن المستخدم، ويمكن استخدام هذه المعلومات لغايات متعددة تجارية، أو دعائية، أو تجسسية.

12- استغلال الملكية الفكرية (Intellectual Property):

الملكية الفكرية هي المنتجات ذات الطبيعة المعنوية أو الفكرية (Harris, 1995). وهناك صعوبة في حماية المنتجات التخيلية أو المعنوية، وغالباً ما تفسر الملكية الفكرية على إنها حقوق الطبع أو النشر وتوابعها من حقوق إنتاج، أو نشر أو إذاعة. وهدف هذه الحقوق هو تقدم المعرفة. إن استغلال المصادر والمنتجات الفكرية، أو سرقتها، أو تخريبها قد يصب في صالح أحد الأطراف في حرب المعلومات، والاستفادة مما لدى الطرف الآخر، وإذا كانت المعلومات في مجال الصناعات العسكرية مثلاً يمكن تطور مضادات عسكرية لهذه الدفاعات أو تطوير نماذج أرخص . . إلخ. وينشط الجواسيس في الحصول على هذا النوع من المعلومات لأغراض دفاعية، أو تسويقية، أو تنافسية، أو عسكرية بحتة (Meyers, 1997).

13- خرق الملكية الفكرية على الإنترنت:

هنــاك أربعـة أنـــواع مـن حـمايـة الملكيـة الفكرية على الإنترنـت وهي حقـوق الطبع، والـعلامـات التـجارية، وبراءات الاختـراع (Patents)، والأسـرار التجـارية (Trade Secrets)

أ ـ **حقوق الطبع**. تحمى غالبية القوانين أعمال التأليف الأصلي من الاستخدام غير القانوني، أو إعادة الطبع غير القانوني، أو التعديل، أو التوزيع، ويحمي كل ذلك حق التعبير عن الأفكار .

ب ـ **العلامات التجارية**. تحمي القـوانين العـلامـات التـجارية، والأسـمـاء، والكلمات، أو الرموز المستخدمة من الشركات لتحديد سلعتها، ومنتوجاتها، وتميزها عن غيرها من المنتوجات.

ج ـ **براءات الاختراع**. تحمي القوانين الاختراعات الجيدة والمفيدة والجديدة مثل العمليات، والآلات، والانتاج . . . إلخ.

د ـ **الأسرار التجارية**. السر التجاري أي معدة أو معلومة تستخدم في العمل وتعطي مالكها ميزات على الآخرين في كيفية معرفتها أو استخدامها (Meyer, 1997).

14- خرق حقوق النشر (Copyright Infringement):

يشمل امتلاك، أو استخدام، أو الادعاء بملكية عمل محمي دون موافقة المؤلف، وعند بيع العمل مقابل مادي لا يتم التعويض المادي المناسب للمؤلف،أو صاحب العمل، أو الجهة ذات حق النشر. وقدرت الخسارة لصناعة النشر الرئيسة الأمريكية في عـام 1996م، بين (18ـ 20) مليـار دولار فـقط إلى القـرصنة خـارج الـولايات المتحدة، وقد قدرت الخسارة كلياً (28) مليار دولار (Operation Center Copy).

ففي دراسة لمؤسسة البحث والتخطيط الدولية (The International Planning and Research Corporation (IPR)). أن خسارة قرصنة برامج الحاسب قد بلغت (11.4) مليار دولار عام 1997م، بيما كانت (11.2) مليار دولار عام 1996م، و(13.3) مليار

دولار عام 1995م، وبصفة عامة فإن حوالي (40%) من برمجيات الأعمال قد تمت قرصنتها، وكانت أعلى نسبة في أوروبا الشرقية وبنسبة (77%). بينما تعد فيتنام من أكثر الدول وبنسبة (98%)، تليها الصين بنسبة (96%)، أما الولايات المتحدة فتعد من أقل الدول التي تعرضت لهذه القرصنة وبنسبة (27%)، ولكن كانت من أكبر الخاسرين وبمبلغ إجمالي وقدره (2.8) مليار دولار.

أما الدول الأخرى ذات النسب القليلة، فكانت بريطانيا وبنسبة (31%)، واستراليا بنسبة (32%)، واليابان بنسبة (32%)، والدنمارك بنسبة (35%)، والمانيا بنسبة (33%)، ونيوزيلاندا بنسبة (34%) (BSA/SPA, 1998).

وفي هونج كونج تباع النسخ غير القانونية من مايكروسوفت أوفس (97) بمبلغ (40 دولار) بالعملة المحلية، وهذا ما يعادل (5دولارات أمريكية)، في حين أن الكلفة الأساسية للرزمة (3899 دولار أمريكي).

15- قرصنة البرمجيات (Software Piracy).

وهي إعادة انتاج غير قانونية لبرمجيات الحاسب سواء كان ذلك للدعاية أو التجارة أو الاستخدام الشخصي. وتقتل قرصنة الحاسب الإبداع في شركات الحاسب، وقد تؤدي إلى إفلاسها، كما إنها تؤدي إلى ثراء جهات لم تبذل جهداً فكرياً ولا مادياً في هذه البرمجيات، وبعضها الآخر خاصة إذا كانت برمجيات ذات تطبيقات عسكرية، أو في مجالات الأسلحة، أو الطيران، أو الفضاء تمثل تهديداً أمنياً كبيراً للدولة ذاتها.

وتعد الصين من أكثر بلدان العالم في قرصنة برمجيات الحاسب، وقدرت فيها نسبة القرصنة بـ(98%)، بخسارة تمثل (500) مليون دولار، وفي عام 1994م قدر عدد الحاسبات بـ(750) ألف حاسب قد بيعت في الصين في عام 1993ـ1994م مع حوالي (1) مليون برمجيات قد تم شراؤها بطريقة قانونية خلال الثلاثة أرباع الأولى من عام 1994م. (Ho, 1995). وتنتج المصانع الصينية (75) مليون قرص مدمج علماً أن الحاجة المحلية كانت (5) مليون ولكنها ذهبت إلى قرصنة البرمجيات والتي صدرت إلى دول أخرى، وفي هونج كونج وحدها، كانت نسبة القرصنة (62%)، وقدرت

بحوالي (100) مليون دولار (Ho, 1995). وتظهر أرقام عام 1994م عن كلفة قرصنة برمجيات الحاسب إنها على النحو التالي :

جدول رقم (15)

تقديرات قرصنة برمجيات الحاسب لعام 1994

الدولة	القيمة بالدولار	نسبة القرصنة
الأرجنتين	208.220.00	%80
استراليا	127.543.294	%37
البحرين	6.940.000	%96
بلجيكا	77.304.687	%46
بوليفيا	12.460.806	%95
البرازيل	550.936.140	%77
بلغاريا	30.900.000	%95
كندا	254.533.200	%58
شيلي	70.414.496	%84
كولمبيا	90.765.000	%81
دول المجموعة الأوربية	10.413.000	%97
قبرص	3.847.500	%91
الدنمارك	89.818.500	%46
الإكوادور	7.013.200	%98
مصر	38.910.344	%85
السلفادور	13.142.700	%97
فنلندا	48.098.063	%43
فرنسا	771.460.734	%57
ألمانيا	1.874.741.352	%50
اليونان	79.231.445	%80
جواتمالا	8.520.000	%94
الهندورلاس	4.652.592	%89
هونج كونج	132.688.75	%62

هنغاريا	101.500.000	%85
الهند	127.527.600	%82
أندونيسيا	118.320.000	%99
إيران	9.798.894	%97
إيرلندا	44.525.803	%82
إسرائيل	42.329.763	%74
إيطاليا	404.382.943	%58
اليابان	2.075.809.729	%67
الأردن	3.382.500	%96
كينيا	647.600	%90
كوريا	545.926.907	%78
الكويت	14.094.000	%99
لبنان	1.607.526	%95
ماليزيا	96.207.600	%89
مالطا	2.916.000	%90
المكسيك	200.213.302	%78
المغرب	23.200.000	%81
هولندا	204.938.610	%58
نيوزيلاندا	105.436.670	%55

المصـــــدر : http:/fabweb.cityu.edu.hk/archive/97-98b/is3532/materials/PIRACY.HTM, Ho, 1995, p. 11.

و تعد سرقة البرمجيات ونسخها وتوزيعها أو إعادة بيعها من الأعمال الرائجة في جرائم الحاسب، وهذه مشكلة دولية، وكانت من المواضيع الهامة في اتفاقية التجارة التي عقدها الرئيس الأمريكي بل كلنتون مع الصين. ويمكن الوقاية من القرصنة من خلال الأساليب التقنية (Shade, 1995)، ويرى تمبلتون أن الحماية القانونية غير ضرورية طالما توفرت الحماية التقنية ضد القرصنة (Templeton, 1997).

16- خرق حماية الاتصالات والبيانات

يشمل خرق حماية برمجيات الحاسب والبيانات التعدي على أو اعتراض، أو استخدام، أو إساءة استخدام، أوالحرمان من الخدمة للاتصالات والبيانات، ويشمل:

1- التعدي على البيانات: هناك عدة أنواع من التعديات على سرية ووحدة ووجود البيانات وسرية البيانات (Confidentiality) والتي تتعلق بحفظ البيانات بعيداً عن تناول يد غير المصرح لهم والمسموح لهم بالاطلاع عليها أو استخدامها. وتكامل ووحدة البيانات (Integrity) تشمل المحافظة عليها دون تعديل من قبل الأشخاص غير المسموح لهم بتعديلها، ووجود البيانات يعني مدى توافرها للاستخدام (Availability)، وهناك مفهومان عند التعامل مع التعديات على البيانات هما:

أـ التخمين أو الاستنتاج (Inference) ويعني استخدام أجزاء بسيطة من البيانات لاستنتاج أو تخمين الباقي أو الكل.

ب- الربط (Linkage) وتعني حصول الفرد على ربط غير شرعي مع البيانات.

ويشمل التعدي على تكامل ووحدة البيانات الأنواع التالية من التعديات:

1 ـ النسخ غير القانوني للبيانات (Un Authorized Coppying of Data) النسخ غير القانوني للبرمجيات (Piracy) نوع آخر يمكن تصنيفه مع هذه الفئة، وقرصنة برمجيات الحاسب نوع آخر من النسخ غير القانوني للبيانات، إن الطريقة في اكتشاف والوقاية من مثل هذه الجرائم سواء كانت نسخ بيانات تتعلق بالأمن أو البرمجيات التجارية أو بيانات تتعلق بالمؤسسات الحساسة، أو بيانات شخصية. والوقاية من هذا النوع من التعديات يتطلب تنسيق سياسات بين فئات متنوعة في أمن المعلومات، ففي مجال السلامة الشخصية فإن تعليم المستخدمين عملية حيوية في مجال أمن عمليات الدخول . . . إلخ.

3ـ تحليل المرور الإلكتروني (الذورة) (Traffic Analysis) : المرور (Traffic) يعني أحد العناصر التي يقيم أداء الخادم (Server) بموجبها، وعندما يرسل الخادم المرور إلى موقعك، فإنه يتوقع أن تنظر إليه كالسير (على الطرقات) الذي بحاجة إلى خدمة، وأن ترسل لهم ما يحتاجونه، أو أن ترحب بهم كزوار لموقعك، وتعاملهم ما يتوجب عليك فعله لهم كضيوف.

ان الخادم الجيد ينشئ سجلاً بكل ما يحصل عليه وهذه تسمى ملفات الدخول (Log files)، ويقوم الخادم بإنشاء ملف كبير بما يحدث عليه. فعندما تطلب صفحة معينة فكأنما تقول للحاسب اذهب للموقع (X) وأحضر لي محتوى الصفحة (Y). والمهم هنا عند تلقي هذا الأمر من الخادم المعني ما يهم هو السؤال : من الذي طلب هذه الصفحة؟ وفي هذه الحالة يسجل عنوانك (IP) الخاص بالحاسب مثل (24.1.164.14)، وهذاالرقم يتغير كل مرة تدخل فيها للانترنت من الاتصال عبر المودم (Dial-up)، (Wilson, 2000).

إن الدخول واستراق السمع لما يقال على الشبكة أو اعتراض ما يرسل يسمى بتحليل الذروة، وهناك الكثير من عمليات التنصت والاعتراض التي تتم من دخلاء أو هواة أو مجرمين وجواسيس وذلك لغايات مختلفة.

4- القنوات المخفية (Covert Channels) : هناك بعض الطرق التي تمكن من إخفاءمعلومات هامة أو كلمة دخول من خلال تغير اسم ملف يبدو عادياً أو تغير محتواه ووضع المعلومات الحساسة فيه (Norman &Neuman, 1992).

5- التعديات على البرمجيات (Software Attacks): هناك أنواع من التعديات على البرامج أهمها طريقة الأبواب الخلفية أو أبواب المصائد (Traps Doors)، وطريق الباب الخلفي تعني طريقة سريعة توصل للبرنامج. إنها تمكن المبرمجين من المرور إلى البناء الرسمي للبرنامج الآن وفي المستقبل، مما يُمكن المُبرمج من تعديل البرنامج.

6ـ اختطاف الحلقة (Session Hijacking): يعني سحب الـ(URL)، وسرقة الحلقة، وتشكل أحد الاهتمامات الأمنية الكبيرة الآن (Joshua, 2000)، وهذا نوع جديد من التعديات في فئة الاتصالات، وهذا يعني أن مستخدماً غير قانوني يستخدم شاشة شخص آخر وهي مفتوحة أثناء غيابه عنها، ومعرفة المعلومات، أو نسخها، أو تغيرها أو مسحها، مما يشكل صعوبة لصاحبها في إعادة استخدامها.

7ـ الالتفاف (Turneling): هو استخدام طريقة قانونية في نقل البيانات غير القانونية (غير المسموح في نقلها أو إرسالها لمكان ما).

8- تعديات التوقيت (Timing Attacks) : وهي طريقة معقدة في الدخول إلى البرمجيات أو البيانات، حيث تتطلب استغلال الوقت الذي يتطلبه النظام في السباق بين عمليتي معالجة، والمخرجات تعتمد على من يفوز في السباق ويمكن أن تحصل هذه العملية من خلال ما يعرف باللاتزامن (Asynchronous) وذلك عندما يقوم النظام بتنفيذ مهمتين أو أكثر في الوقت ذاته مما يتيح المجال أمام المبرمج للدخول إلى البيانات وتعديلها (Kocher, ND).

17ـ **خرق الخصوصية** (Privacy)

لا تتوقف الخصوصية كما وصفها عند المعلومات، فحق الفرد في أن يوجد وحده أو مع أسرته أو في أي مكان، وليس مكشوفاً للعروض الهجومية والحق في أن لا تراقب سلوك الناس (كالتنصت، أو العيون الإلكترونية)، وبالتالي فإنه يمكن النظر إلى الخصوصية بأنها تشمل المجال الفيزيقي والمعنوي والمعلوماتي للفرد الذي يخترق أو ينتهك دون إذن منه.

وأحد المخاوف التي أظهرتها استخدامات الحاسب من الناحية القانونية هو أن قواعد المعلومات التي بنتها مراقبة الحكومة من الممكن أن تستخدم في نشاطات قانونية أو غير قانونية مزعجة وتتعدى على خصوصية المواطن. هذا بالإضافة إلى ظهور تجارة بيع المعلومات، وبيع العناوين إلى وكالات وشركات التسويق والتي تخرق خصوصية الأفراد، وتمطرهم بالدعايات من خلال البريد الإلكتروني. وكاستجابة لذلك زادت القوانين التي وضعتها الدول في مواجهة مثل هذه الانتهاكات، وظهرت قضايا جدلية مثل حرية المعلومات والتي قد تتعارض مع الخصوصية (البداينة، 2000). ومن البرامج التي وافقت وزارة العدل الامريكية مع استخدامها برنامج المفترس المخصص لاختراق البريد الالكتروني والانترنت والتجسس على الأفراد وخاصة من قبل ال (FBI).

18- **الكعكات** (Cookies):

تُعد الكعكات من مهددات الخصوصية على الإنترنت والكعكات هي المعلومات التي يرسلها الموقع على الإنترنت إلى حاسبك عندما تتصل بذلك الموقع وعند تلقي هذه المعلومات فإن حاسبك يحفظ هذه المعلومات على القرص الصلب، وفي كل مرة

تزور ذلك الموقع فإن المعلومات ترسل للموقع. وتسمح الكعكات للموقع بوضع معلم فريد محدد إلى ذلك الحاسب والذي يستخدم ليرتبط مع الطلب المقدم إلى الموقع من ذلك الموقع سابقاً، ولكن إذا أظهرت معلومات معينة على ذلك الموقع فإن الكعكات يمكن أن تكون عنك صفحة ما تحتوى هواياتك ومشترياتك ويمكن استخدامها عند ذلك لغايات التسويق. ويمكن مكافحة الكعكات بالآتي :

1ـ وضع ملف الكعكات على قراءة فقط، وهذا يعتمد على نظام التشغيل، أو المتصفح المستخدم.

2ـ إعداد الحاسب بحيث تحذف الكعكات كل مرة عند بداية تشغيل الحاسب.

3ـ استخدام برامج خاصة بالكعكات مثل (Cookic Cutter)، أو (Cookie Crusher).

الفصل الثامن

العمليات النفسية وادارة النفس والادراک

مقدمة

تعني العمليات النفسية (Psychological Operations)، العمليات المخطط لها لتمرير معلومات منتقاة ومؤثرات لمستمعين أجانب للتأثير على عواطفهم، ومعتقداتهم، ودوافعهم وتبريراتهم الموضوعية، وسلوكياتهم، وبشكل كبير على سلوك الحكومات الأجنبية والمنظمات، والجماعات، والأفراد.

وتهدف العمليات النفسية (Psyop) إلى إغراء، أو تعزيز الاتجاهات الأجنبية، والسلوكيات المحببة لأهداف المرسل. وعند تطبيق العمليات النفسية فإنها تضعف الروح المعنوية وتخفض الفاعلية لقوى العدو. وقد تؤدي إلى عدم الطاعة، وإلى اللاتعاطف عند هذه الأطراف. وتعد العمليات النفسية جزءاً من النشاطات السياسية والاقتصادية والمعلوماتية لبلدان معلوماتية مثل الولايات المتحدة الأمريكية.

تظهر الأقول التالية الأهمية العالية للعمليات النفسية، فيقول جيلدار «إن أغلى رأسمال هو رأسمال العقل والروح البشرية» (Gilder, 1989, p. 12). أما ستين فيقول: «إن هدف حرب المعلومات هو العقل البشري خاصة العقول التي تتخذ قرارات الحرب والسلام» (Stein, 1998, 1996).

والعمليات النفسية من أقدم الأسلحة المستخدمة في الحرب، وتعرف العمليات النفسية (Psychop)، أو الحرب النفسية (Psywar) هي ببساطة أن تعرف كل شيء عن عدوك. تعرف معتقداته، ورغباته، وقوته، وضعفه، وانكشافاته (الثغرات). عندما تعرف الدوافع التي تحرك خصمك تكون جاهزة لبدء الحرب النفسية. العمليات النفسية هي الاستخدام المخطط للاتصالات للتأثير على الاتجاه والسلوكيات البشرية، سلوكيات وعواطف، واتجاهات في الجماعات المستهدفة تدعم تحقيق الأهداف الوطنية. أما طريقة الاتصالات فيمكن أن تتراوح بين نشر معلومات من خلال الدعاية (كلمة تنقل)، أو من خلال وسائل الإعلام. إنها حرب العقل (A War of Mind). الأسلحة الرئيسة فيها هي النظر (Sight)، والصوت (Sound). ويمكن نشرها بالاتصالات أو الوسائل المرئية (المنشورات، والصحف، والكتب، والمجلات، والعروض). فالسلاح هنا ليس بالوسيلة التي تحمله، ولكن بالرسالة التي يحملها وكيف تؤثر في المُتلقي.

قال صن توز (Sun Tuz): «إن الاستيلاء على جيش العدو بأكمله أفضل من تدميره، ولكي تفوز مئة مرة في مئة معركة، فإنه ليس قمة المهارة اخضاع العدو دون قتال، بل إنه الامتياز الأعلى(Supreme Excellence). وبالتالي فإن من الأهمية بمكان في الحرب هو محاربة استراتيجية العدو، وثانياً تخريب (Disrupt) حلفائه بالدبلوماسية والأفضل تالياً هو مهاجمة جيشه وأسوأ سياسة أن تهاجم المدن» (انظر ، Carlson,1997، وDevostt,Houghton,1997، وEverett,et.al.,1997، وFast,1997، وFox,1997، و Fredericks,1997، وMiller,1997، و(Neilson, 1997).

والأمثلة التالية تبين أهمية انتقاء الكلمات: كيف تشعر وأنت ترى علم بلدك يرفرف؟ وما شعورك عند سماع النشيد الوطني؟ ما رأيك «ليحفظ بلدي» . الصوت والموسيقى عاملان هامان في دفع العواطف إذا اقترنت بالرسالة المناسبة. لقد قيل إن القلم أقوى من السيف، وذلك إن استخدم بشكل مناسب، فإن الكلمات تدخل لإثارة طموح ودافعية الآخرين، والجمل التالية تبين ذلك:

«أعطني الحرية أو الموت»

«أعتذر لأن لي حياة واحدة لأعطيها لبلدي».

«لا تسأل مايمكن أن تفعله بلدك لك بل اسأل ما يمكن أن تفعله انت لبلدك».

لقد استخدمت العمليات النفسية بكثرة في الحرب العالمية الثانية، وركز الألمان وخاصة هتلر على إظهار عدم رضا المؤيدين للجناح التقدمي اليساري واليمين من خلال تركيزه على فشل هذه الأحزاب في حل المشكلات الناجمة من الظروف المفروضة على ألمانيا، ومن ثم تقدم باسم الشيوعية الوطنية لحركة واحدة قادرة على توحيد البلاد، ومركزاً في خطاباته على الفخر والوحدة ووضع اللوم على أعداء ألمانيا.

أنواع العمليات النفسية

هناك أربع فئات من الحرب النفسية العسكرية هي :

1ـ العمليات النفسية الاستراتيجية (Strategic Psyop) وهي نشاطات معلوماتية دولية تقوم بها الدولة للتأثير على اتجاهات الخصم وإدراكاته وسلوكياته باتجاه محبب لتلك الدولة وأهدافها، وعادة ما تنفذ هذه البرامج خارج الدولة وخارج النطاق العسكري.

2- العمليات النفسية العملياتية (Operational Psyop). وعادة ما تنفذ قبل الحرب وخلالها وأيام الصراعات، وقد تكون موجهة لبقعة جغرافية معينة اثناء الصراعات المفتوحة.

3ـ العمليات النفسية التكتيكية (Tactical Psyop). وتنفذ في منطقة لقائد تكتيكي خلال الصراعات أو الحرب لدعم هدف تكتيكي ضد الخصم.

4ـ العمليات النفسية التماسكية (Consolidated Psyop). وتنفذ في المناطق الأجنبية العدائية والتي تكون محتلة من طرف الدولة، ويوجد فيها خصم أو جماعات عدائية للدولة، وتنفذ لانتاج سلوكيات مؤيدة وداعمة لأهداف الدولة.

وتهدف الأنواع الأربعة من العلميات النفسية إلى خفض الروح المعنوية وفعالية القتال داخل الرتب العسكرية لدى العدو، وخلق فوضى وعدم ثقة بين أفراد العدو، وحمايتها من عمليات الخداع والتأثير المضاد، وتوفير التعاون والوحدة، والروح المعنوية لدى قواتنا والحلفاء ومع المقاومة خلف خطوط العدو (Fulford, 1996).

مبادئ العمليات النفسية

هناك عدد من المبادئ التي تحكم العمليات النفسية وهي على النحو التالي:

1ـ الزمن: يمكن أن تكون العمليات النفسية قصيرة الزمن أو طويلة الزمن للتأثير على الخصم ودعم القوة والجيش.

2ـ الهدف: يجب أن يكون هدف العمليات النفسية محدداً وواضحاً.

3ـ الفعاليات: يجب أن يكون موضوع العمليات النفسية ونشاطاتهاورموزها مبنية على تحليل الهدف بما في ذلك الإمكانات الصديقة والعدوة ومناطق القوة والضعف.

4ـ يجب تقييم جميع الأعمال العسكرية من حيث مضامينها النفسية، وإمكانية دعمها للأفعال النفسية المقصودة لكي يتجنب آثارها السلبية وتعزيز آثارها الإيجابية.

5ـ يجب أن تكون وسائل الإعلام المختارة لنقل العمليات النفسية موثوقة وأن تكون ممكنة الوصول من قبل الجمهور المستهدف.

6ـ الاستغلال السريع للمواضيع النفسية غالباً ما يكون حرجاً. إن تخطيط الإجراءات، والفحص القبلي، والموافقة على الإجراءات يجب أن تكون مطورة لاستغلال عمليات الزوال.

7ـ يجب تقييم نتائج العمليات النفسية دائما كلما أمكن ذلك لمعرفة مدى صلتها بالهدف الأصلي والأهداف الوطنية والعسكرية.

8ـ تؤثر العمليات النفسية في الذين يقاتلون في الميدان، وبالقادة العسكريين والجنود، والقادة السياسيين، والجمهور المدني (Fulford, 1996).

والواقع كما نجده يتحدد بما ندركه ـ ما نسمع ونرى ونخبر. إن تفسيرنا لهذه المدركات يؤثر في الأفعال التي نتخذها من شراء السيارة إلى إعلان الحرب.

ويميز وود (wood) بين الحرب النفسية (psywar) والعمليات النفسية (psyop) على أن الحرب النفسية تعني الاستخدام المخطط للدعاية وللأفعال النفسية الأخرى بقصد التأثير على آراء وعواطف واتجاهات وسلوكيات الاعداء بطريقة تحقق الأهداف الوطنية. أم العمليات النفسية فهي العمليات المخططة لتمرير معلومات معنية ومؤشرات الى مستمعين أجانب للتأثير على عواطفهم ودوافعهم وتقديرهم وسلوك الحكومات الأجنبية والمنظمات والجماعات والافراد والقصد هو تعزيز أو إغراء سلوك الأجانب أو اتجاهاتهم المحببة لأهدافنا (Wood,ND).

إدارة النفس والإدراك

تعني إدارة النفس والإدراك عمليات المعلومات الهادفة إلى التأثير في إدراك ونفس الآخرين بقصد التأثير على عواطفهم وتبريراتهم (السلبية)، وقراراتهم وبالتالي أفعالهم. إنها مرتبطة بالعمليات النفسية والتي تهدف إلى التأثير على السلوك من خلال التأثير على نفسية الفرد من خلال الخوف والرغبة والمنطق والعوامل العقلية الأخرى. وقد تكون موجهة إلى فرد أو جماعة أو مجتمع.

تصل العمليات العدوانية إلى عقول المجتمع من خلال المحتوى في المجال المعلوماتي المجتمعي، والوصول إلى المجال المعلوماتي المجتمعي يكون من خلال وسائل الاتصال، وأي وسيلة اتصال يمكن أن تستغل بما في ذلك الاتصالات وجهاً لوجه، والاتصالات المطبوعة، والبث، والشبكات. وتعني إدارة النفس والإدراك

الانتقاء الإعلامي الجيد أو الرديء للتأثير على الآخرين. ومن أمثلة وسائل الاتصال في الوصول إلى المجتمع التلفزيون، الكثير من الناس يشاهدون التلفزيون أكثر من أي وسيلة أخرى، حيث التغطية الدولية الكبيرة للأحداث.

لقد حدد الفن وهايدي توفلر ست أدوات في هجومية ودفاعية.

1ـ الاتهامات الوحشية (الصحيحة والكاذبة) (Atrocity Accusations) من مثل قصة حاضنات الأطفال الكويتيين التي أُتهم الجيش العراقي بقتلهم إبان حرب الخليج.

2ـ تضخيم الدعاية (Hyperbolic Inflation): مثل وعود الرئيس بوش بأن حرب الخليج هي من أجل نظام عالمي جديد.

3ـ سلاح الدعاية (Propaganda Weapon) : وهي تستخدم خاصة في التحقير (Dehumanization) أو / الشيطنة (Demonization). وكما وصف الرئيس العراقي أمريكا بالشيطان الأكبر، وصف الرئيس بوش الرئيس العراقي بهتلر.

4ـ الاستقطاب (Polarization)، إذا لم تكن معنا فأنت ضدنا. وهذا ما استخدمه بوش الابن في حربه على الارهاب عقب احداث 2001/9/11، من ليس معنا فهو مع الارهاب.

5ـ العقاب الإلهي (Divine Sanction) من مثل طلب بوش مساعدة الرب.

6ـ إبطال الدعاية (Meta-Propaganda) وهي الدعاية التي تبطل مفعول الدعاية المضادة (Toffler &Toffler, 1993).

يمكن أن تكون الصور والأصوات أدوات مؤثرة في العقل، ففي1996/12/16م، فقد سبب برنامج تلفزيوني بث في اليابان بأن آثار نوبات (Seizures) من التشنج في مئات الأطفال حيث عانى أكثر من (600) طفل من التشنج، والتقيؤ، واحمرار العيون، واعراض أخرى بعد مشاهدتم برنامج البوكيمون (Pokemon) برنامج الاطفال التلفزيوني الشهير.

وقد أدخل المستشفى أكثر من (100) طفل، وحدثت نوبات من خلال مسرح الكرتون من خلال تفجير «قنبلة تطعيم» اتبعت بعد تسليط ضوء أحمر في عيون بوكاشو (Plkachu) حيث إن هذه الأعراض يمكن إثارتها من خلال تسليط الأضواء الملونة.

وسائل العمليات النفسية المعلوماتية:

ويمكن تحديد الوسائل التالية في حرب المعلومات الهجومية، والخاصة بإدارة النفس والإدراك:

1ـ **الكذب** (Lies).

الكذب أحد أدوات إدارة الإدراك والتي تهدد مصداقية الناقل الإعلامي للكذب. وهذا يشمل المواطنين الذين يعتمدون على الإعلام كمصدر للمعلومات أو أولئك المهتمين بالمعلومات والذين يؤذون من نشر الكذب (Falsehoods). وأحياناً تقوم الحكومات بنشر دعاية كاذبة عبر التلفزيون وفي الوقت ذاته تراقب وتحرر ما ترغب به وتمنع من ظهور اتجاهات مضادة لموضوع الدعاية، وفي عصر المعلومات سهلت التقنية الرقمية عملية فبركة (Fabrication) أو تزوير المعلومات. فالوثائق يمكن أن تنشأ وينتقي تحريرها، والأشرطة يمكن قطعها وتوصيلها معاً، والصوت يمكن انتقاء المقاطع وتكوين الكلمات التي لم يقلها الشخص. وعلى الرغم من أن وسائل الاتصال يمكن ترقيعها وتزويرها إلا أن الناس يثقون بما يرون (Denning, 2000 b). ويستخدم الكذب للتأثير على معنويات الناس، أو تغيير اتجاهاتهم، أو دعم موقف معين سياسي أو اجتماعي،ويكثر استخدام ذلك في الحروب لخفض الروح المعنوية عند العدو من خلال المبالغة في خسائره، ورفع الروح المعنوية للطرف الآخر من خلال إبخاس الخسائر.

2- **التشويه** (Distortion)

هناك عدة طرق يمكن تشويه المعلومات بها وعن قصد، فيمكن حجب عناصر أو معلومات مهمة أو إيقافها، أو حذفها، أو تحريفها. يمكن أن تستخدم المعلومات بطرق مضللة، يمكن عرض جزء ما وإهمال الجزء الآخر. ومن الأمثلة على ذلك في عام 1997م أذاع التلفزيون اليوغسلافي أبان حرب البوسنة شريطاً محرفاً من الأخبار عن مؤتمر صحفي قدم من المدعى العام للأمم المتحدة لويس أربور (Louise Arbour) وكان المذيع الاكسندر ايفنكو (Alexander Ivanko) والذي يدعم الرئيس رادوفان كرادزك (Radovan Karadzic) قد قطع عبارات المدعي العام واحل محلها تعليق «التحرك ضد الغرب» والانتقال من مؤسسة قانونية إلى إدارة سياسية تهدف لوضع الضغط على الغرب» وصوت خلفي يصف الرئيس بأنه بطل. أما الشريط الأصلي فقد

طالب اربور (Arbour) باعتقال الرئيس كرادزك، وقال إنه يجب أن يحاكم على المجازر والجرائم ضد الإنسانية.

3ـ **التحريف** (Fabrication):

تقوم المؤسسة العسكرية بتحريف الحقائق والمعلومات وفبركة الكذب للحصول على ميزات ضد العدو. ومن الأمثلة في الحرب العالمية الثانية ما قام به الانجليز في خداع الألمان في الابتعاد عن سيسلي(Sicily) بعد هزيمة الألمان في شمال أفريقيا، أصبحت سيسلي أفضل موقع لغزو أوروبا، والمشكلة الوحيدة لدى الألمان هي تحصين سواحلها الجنوبية. وجاءت الفكرة الإنجليزية بوضع أوراق معطنة (Bogys) في جثة شخص هالك من المتوقع أن يقع في أيدي الألمان، وقد وضعت الجثة كما لو كانت احترقت من تحطيم طائرة في البحر، أوراق مزورة لهوية، وطلبات تحويل، ونقود، ورسائل، وصور لصديقة، وفواتير غير مدفوعة. ولقد سبحت الجثة، ووصلت إلى الأسبان وسلموا المعلومات للألمان وهي تحمل الأوراق، بأن هناك هجومين للحلفاء على سردينا وكلاماتا، وبعد بدأ الألمان بوضع الالغام في البحر تجاه كلاماتا بدلاً من سيسلي، وهذه العملية انقذت حياة مئات الآلاف من الأمريكان والإنجليز (Yeo & Hillo, 1954) (Motague 1954).

ومن الأمثلة المروعة في هذا المجال في 1980/6/3م، قام الكولنيل وليام أودوم (Odom) المساعد العسكري لمستشار الأمن القومي زبجينو برجينسكي (Brgezinski) قد أفاق رئيسه منتصف الليل لإعلامه أن الروس قد أطلقوا (200) صاروخ على الولايات المتحدة، وأراد برجينسكي أن يتأكد من أن القنابل الأمريكية جاهزة للرد المضاد، وعلم أن (NORAD) يذكر أن (2200) قد أطلقت في هجوم شامل، وكان برجنيسكي على وشك إعلام الرئيس الأمريكي جيمي كارتر، وتبين أن فلماً من المناورات العسكرية قد غذي للحاسب (NORAD) بالخطأ (Associuted Press, 1997).

4ـ **الفسوق** (Hoaxes) :

الفسوق هو قصص ملفقة، القصد منها التسلية أو إثارة الخوف، ويعد الإنترنت من أفضل الأمكنة لنشر قصص الخوف، فخلال دقائق تصل القصة الكاذبة إلى آلاف

الناس، وبمختلف المواضيع، وخاصة مواضيع الفيروسات أو القصص الكاذبة حول الأشخاص أو الشركات لتدمير سمعتها. الخداع في انتقاء المعلومات، ويهدف إلى تكوين معلومات مضللة لإرباك طريق العدو في الحياة، وانهيار البناء الاقتصادي له، وتحجيم قدراته على اتخاذ القرار، وحفض فعالية قواته العسكرية.

5ـ **الخداع** (Deception):

يعد الخداع متعدد الأشكال، ويستخدم مع جميع العمليات العسكرية، وقديما وقبل حوالي (2500) سنة، ذكر صن تزو (Sun Tzu) في كتابه الشهير «جميع الشؤون الحربية مبنية على الخداع» ويرى بأن جميع الشؤون الحربية قائمة على الخداع (Deception)، ويقول: عندما نكون قادرين على الهجوم يجب أن نبين أننا غير قادرين، وعند استخدام قواتنا، يجب أن نظهر بأننا غير فاعلين وعندما نكون قريبين يجب أن نجعل العدو يعتقد أننا بعيدين جداً، وعندما نكون بعيدون جداً يجب علينا أن نجعله يعتقد أننا قريبون جداً» (Neilson,1997). كما أن قصة حصن طروادة معروفة وتتراوح أعمال الخداع من البسيط، أشرطة مج (Mig) في فيتنام إلى غزو نورماندي (Normandy).

طبقت خدعة «جراب المؤونة» (Haversack) في عام1917م في الحرب بين الانجليز والأتراك في فلسطين، وكان لواء إنجليزي يُدعى منيهيرتزهاجن (Menihertzhagen) قد خدع الأتراك بجعلهم يعتقدون أن الهجوم الإنجليزي سيكون انزالاً ثنائياً (Amphibious) في غزة في4/11 في الوقت الذي كان فيه الهجوم الحقيقي سيكون في بيرشيفع في10/3. وقد قام اللواء بتوزيع بيانات خاطئة في رسالة مشفرة بعد أن سمح للأتراك بحل أحد رموز الراديو وبقصد فقد جراب مؤونته الذي يحوي وجبة الغداء ملفوفة بوثيقة رسمية تؤكد الهجوم في 11/4 على غزة، ويبعد الأنظار ويؤكد الخدعة فقد بذل جهداً كبيراً في البحث عن جراب مؤونته، مما جعل الاتراك ينقلون جنودهم إلى المكان الخطأ في 10/3، وكان خط المعركة الذي حصن لأشهر قد تم اجتيازه من الإنجليز في 11/9 وكانوا في القدس (Fowler & Nesbit, 1995).

ولكي ينجح الخداع لابد من ملاحظة الخداع من قبل العدو، وتحليل الخداع كواقع، والفعل بناءً على الخداع وفق أهداف الخادع (Fogleman & Widnall, ND). لقد استخدام المصريون الخداع «الأشراط» كنوع من الخداع ليتمكنوا من مفاجأة

الاسـرائيلين في عـبـور القناة عـام 1973م. ولعـدد من السنين دأب المصـريون على التدريب المتكرر، حيث تجهز الاسرائيليون له في البداية، وبعدها تكونت لديهم قناعة بأن ذلك تدريـب روتيني دفـاعي. وقد تمـت الاسـتعـدادات المصرية في عـام 1973، وكانت تحت غطاء تدريبات روتيتية دفاعية، وجعل الاسرائيليين يعتقدون أن المصريين يقومون بذلك كإجراءات دفاعية وأنهم يخشون انتقام اسرائيل لحادثة ميونخ. ولقد سهل هذا الخداع عبور المصريين للقناة وتحقيق مفاجأة لدى الاسرائيليين.

6ـ الهندسة الاجتماعية (Social Engineering):

تعني الهندسة الاجتماعية اكتساب المعلومات الحساسة، أو ميزات الوصول غير المناسبة من قبل الخوارج بناءً على إقامة علاقات ثقة غير ملائمة مع الداخليين. إنه فن انتقاء الأفراد ليفعلوا أشياء ماكان ليفعلوها في الوضع الطبيعي، والهدف هو خداع شخص ما لتقديم معلومات قيمة، أو وصول للمعلومات، ويركز على الطبيعة البشرية مثل الرغبة في المساعدة، أو الرغبة في الثقة بالآخرين، والخوف من الوقوع في المشاكل، ومؤشر الهندسة الاجتماعية الناجحة هو الحصول على المعلومات دون إثارة الارتياب (Tims, 2001).

وتعني حصول الدخلاء على تقليد المستخدمين الشرعيين ليتمكنوا من الدخول غير الشرعي إلى نظم الحاسب. ويستخدم الدخلاء الهندسة الاجتماعية في إظهار على أنهم هم من العاملين في المؤسسة ويخدعون الآخرين ويحصلون على معلومات عن الحاسب، أو البريد الإلكتروني، أو من خلال الزيارة الشخصية.

تعني الهندسة الاجتماعية العمليات التي تجعل الآخرين يقومون بفعل ما، ليس من الممكن أن يقوموا به لو عرفوا الحقيقة. أي وسيط بين اتصال فرد ـ فرد يمكن أن يستغل هذا الاتصال. قد استخدم هذا المصطلح النازيون ليعنوا به عمليات انتقاء المجتمع كاملة. واستخدمه الروس، وفي الثمانينات استخدمه الدخلاء غير الشرعيين للحاسب (Hackers) لوصف استراتيجياتهم في الحصول على المعلومات بأسس غير تقنية (Winkler, 1977).

إن غالبية الناس يعتقدون أن الدخول للحاسب يتطلب شخصاً محترفاً فنياً، إنه نتيجة التدفق المعلوماتي الكبير فقد تمكن الدخلاء من استغلال هذه المعلومات. والواقع أن الهندسة الاجتماعية تمكن الدخلاء من خرق أمن المعلومات.

ويمكن تصنيف الهندسة الاجتماعية إلى نوعين هما الهندسة الاجتماعية البشرية، والهندسة الاجتماعية الحاسوبية، وتعني الهندسة الاجتماعية البشرية التفاعلات (فرد ـ فرد) للحصول على المعلومات المرغوبة. أما الهندسة الاجتماعية الحاسوبية فتعني استخدام برامج الحاسب في الحصول على المعلومات المرغوبة. وتشمل الهندسة الاجتماعية البشرية الأشكال التالية :

1ـ الانتحال (Impersonation). وهو قيام شخص بالادعاء، ويمثل أنه موظف جديد يطلب المساعدة، ويدعي أنه نسي كلمة الدخول، ويطلب من الاستعلامات أو طاولة المساعدة إعادة تجهيز ذلك له لأخذ كلمة جديدة. وفي هذه الحالة يكون لدى الدخيل معلومات كافية عن الشخص الذي يمثله.

2ـ المستخدم المهم (Important User). ولكي يحصل الشخص على المعلومات بسرعة، فإن إدعاءه بأنه مساعد الرئيس يعجل ويسهل في حصوله على المعلومات وخاصة وأن موظف المساعدة لا يتوانى عن تقديم المطلوب لمساعد الرئيس.

3ـ الطرف الثالث (Third Party). ويمكن للهندسة الاجتماعية استخدام اسم طرف ثالث له صلاحيات الحصول على المعلومات، وقد يقول إن فلاناً قد طلب مني الاتصال بكم للحصول على كذا قبل أن يسافر.

4ـ الدعم الفني (Tech Support). ويمكن للهندسة الاجتماعية استخدام وتمثيل دور الداعم الفني الذي يرغب بمعاينة الأجهزة والبرامج بموجب العقود أو أنه قادم بناءً على طلب الإدارة.

5ـ الدخول الشخصي (In person). ويمكن للهندسة الاجتماعية الدخول كشخص يرتدي الزي الرسمي للمؤسسة، أو كضيف أو كعامل خدمات، ويمكن تعيين موظفي النظافة للبحث عن المعلومات المهمة في الشركة.

6ـ البحث في القمامة (Dumpster Diving). وهو البحث في القمامة الخاصة بالشركة المستهدفة.

7ـ النظر من خلف الكتف (Shoulder Surfing). النظر من كتف الشخص لمعرفة ما يطبع أو ما أمامه من معلومات.

أما الهندسة الاجتماعية الحاسوبية فتشمل الأشكال التالية:

1ـ النوافذ النازلة (Popup Window). يظهر على الشاشة نافذة أحياناً تعلم المستخدم أنه فقد الاتصال مع الإنترنت مثلاً، وأن عليه الدخول مرة أخرى (كتابة اسم المستخدم وكلمة المرور). ويكون هناك برنامج قد تم تحميله لينقل معلومات المستخدم ويرسلها إلى حاسب الدخيل.

2ـ مرفق (ملحق) البريد (Mail Attachment). ويمكن إخفاء البرامج في ملحقات البريد الإلكتروني، والتي يمكن أن تنشر الفيروس وتدمر الشبكات، وهذا يشمل الفيروس، والديدان، وحصن طروادة، وعادة ما تحمل الملحقات عناوين جذابة مثل «أحبك».

3ـ بريد القمامة (Spam)، ورسائل السلة(Chain Letters)، والخداع(Hoaxes) كلها تعتمد على الهندسة الاجتماعية في الانتشار.

4ـ مواقع الشبكة(Web Sites). إن توفير شيء مجاني، أو فرصة في الربح من الأشياء الجذابة، ولكي يتم ذلك يطلب الهندسة الاجتماعية البريد الإلكتروني للشخص، غالبية الناس يضعون كلمة المرور هي ذاتها اسم المستخدم (Tmis, 2001).

وفيما يلي أحد الحالات للدخول غير الشرعي باستخدام الهندسة الاجتماعية، لقد مثل الدخيل أنه من قسم العلاقات العامة فقام بالاتصال بسكرتيرة الرئيس وتمكن من الحصول على الرقم الوظيفي للمدير التنفيذي، وفي المكالمة الثانية استغل معرفته برقم الرئيس ليحصل على رقمه في مركز الكلفة والذي يستخدم في المساء لتلقي الإرساليات الخاصة بالشركة للهواتف الداخلية للشركة. ولقد اتصل الدخيل بالمكتب كموظف جديد، وتمكن من الحصول على قائمة بالموظفين الجدد. ولقد طلب الدخيل من الموظفين الجدد أنه سيعطيهم دورساً في الوعي الأمني للحاسب عبر التلفون، وخلال هذه العملية تمكن من معرفة أنوع الحاسبات المستخدمة والتطبيقات وأرقام الموظفين وأسماء المستخدمين وكلمات المرور. وباستخدام (War Dialer) تمكن الدخيل من معرفة رقم الهاتف المستخدم في الإنترنت الخاص بالشركة، وبعدها تمكن من الدخول إلى نظم الشركة واستخدام الأرقام وأسماء المستخدمين وكلمات المرور.

وعامة فإن الهندسة الاجتماعية تقوم على انتحال شخصية موظف جديد لا يعرف بالنظام ولا بالحاسب، فيقوم بالاحتكاك بالموظفين، أو الإدارة لطلب المساعدة. وإن هذا الشخص (المنتحل للشخصية) لا يتذكر اسم الاستخدام، أو كلمة المرور وأنه في حاجة ماسة للدخول للنظام، ويمثل الدخيل هنا دور الشخص الهام (VIP) في الشركة لاخافة الإدارة لحصوله على ما يطلب. ولذلك لا ينصح مساعدة أي شخص إلا بعد التحقق من أنه الشخص الرسمي، ولا تقدم أية معلومات عن حاسبك، أو أي حاسب آخر أو عن الشركة، أصر على التأكد من هوية المتصل، ولابد من التأكيد على حساسية كلمات المرور التي يجب أن لا يعرفها غيرك، وعند الاستعانة بخبراء من خارج المؤسسة فيجب مرافقتهم حتى الانتهاء من العمل من قبل الإدارة (Guttman, Forey & Malking, 1988).

7ـ الشجب (الانتقاد العلني) (Denouncement) :

يشمل الشجب أو الانتقاد العلني رسائل تشويه، أو تقليل من الشأن، أو تحقير شخص الخصم، وتهدف إلى سحب الدعم عن الخصم، أو كسب مجادلة، أو برامج، أو المضايقة، أو بإثارة الكراهية والاتهامات. ويمكن أن تكون بناءً على دعايات أو كذب، ونظريات المؤامرة شكل من هذه الأشكال، وخطابات الكراهية شكل آخر، وهي شائعة بين المرشحين في حملات الانتخابات، ويقع بعضها تحت ما يسمى الدعاية السلبية أي أن الخصم يركز على الصفات السلبية لخصمه بما فيها إثارة الفضائح والمخالفات أو المشكلات مع القانون مثل تعاطي المخدرات في مرحلة عمرية معينة للخصم.

أ ـ نظرية المؤامرة (Conspriacy Theory): يعد الانتقاد العلني صيغة من نظرية المؤامرة، حيث تتناول وسائل الإعلام موضوعاً ما وتركز الانتباه عليه لإبخاس جماعة معينة. فبعد مقتل الأميرة ديانا في عام 1997م، انتشرت الدعايات في رومانيا أن الموساد الإسرائيلي خلف العملية، حيث تقول الدعاية إن الإسرائيلين لا يرغبون أن تكون أم الملك المستقبلي لبريطانيا متزوجة من عربي.

وبعد تحطيم طائرة (TWA) الرحلة 800 عام 1996م، انتشرت دعاية تقول إن البحرية الأمريكية قد أسقطت الطائرة. وفي دراسة مسحية للواشنطن بوست (Washington Post) عام 1997م بينت أن (39%) من العينة يعتقدون أن البحرية

الأمريكية قد اسقطت الطائرة، وأن (50%) من العينة يعتقدون أن استخبارات أجنبية من كواكب أخرى زارت الأرض يحتمل أن تكون هي السبب.

ب ـ القذف (تشويه السمعة الشخصية) (Defamation): القذف أو الافتراء أو تشويه السمعة الشخصية جزء من العمليات النفسية التي تهدف إلى تدمير سمعة واسم الطرف الآخر من خلال نشر معلومات كاذبة عنه، وقد تأخذ شكل الافتراء (Slander) أو الطعن (Libel) حيث يركز الافتراء على الاتصالات الشفوية فيركز الطعن على الكتابة. ويشمل تشويه السمعة الشخصية إلى الكراهية والسخافة (Ridicule)، والحقد (Contempt). فقد تدمر علاقات ذلك الفرد مع الآخرين، إن الطعن والافتراء غير محمية قانونياً في كثير من الدول، ولذا يمكن أن تستخدم للإضرار بالآخرين.

وتعد الإنترنت وسيلة فعالة في الطعن، حيث إن أي شخص يمكن أن يترك أو يعلق (Post) أي شيء إلى القراء حول العالم، وإحدى النتائج هي أن السمعة الشخصية قد تدمر بضغط مفتاح من لوحة المفاتيح. ومن القضايا في هذا الموضوع ما ربحه الأسترالي (40.000) دولار ضد عالم الأنثروبولوجيا شوه سمعته الشخصية في علم الانثروبولوجيا بوضع رسالة أخرى على أحد خدمات الإنترنت الدولية حيث تقول الرسالة «إن مهنته وسمعته مبنية على قدرته على العنف والاستبداد وإنه متخلف» وإنه قد انغمس في سلوكيات جنسية مع الأطفال» (Lang, 1994).

8ـ التحرش (المضايقة) (Harassment)

التحرش أو المضايقة عملية نفسية موجهة للشخص مباشرة، فترسل الرسائل غير المرغوبة للشخص أو «الهدف» مباشرة أو من خلال وسيط مثل التلفون أو البريد الإلكتروني. وعادة ما يكون مشاهير المجتمع عرضة لمثل هذه الافعال. وكذلك تُعد رسائل التهديد بالقتل أحد أشكال التحرش. ففي عام 1997 أرسل طالبان من نيوهامشير رسائل تهديد بالقتل للرئيس الأمريكي السابق بل كلنتون وقد اعترضا من مكتب التحقيقات الفدرالي (FBI)، ووكالة المخابرات الأمريكية (CIA)، وتم تحديد الطالبين وتم فصلهما من المدرسة لمدة شهر ومنعا من استخدام الحاسب لمدة سنة (Reuters, 1997).

وكذلك فإن ما يعرف برسائل البغض (الكراهية) (Hate - emial) قد انتشرت في الإنترنت من خلال البريد الإلكتروني، ففي أحدى الجامعات الهندية أرسلت (700) رسالة من هذا النوع إلى الطلاب الآسيويين تطلب مغادرتهم البلاد، وكذلك رسائل المضايقات الجنسية (Sexual Harassment) منتشرة جداً في الإنترنت. وكذلك القنابل البريدية والتي هي كم هائل من الرسائل المرسلة إلى عنوان ما مما يؤدي إلى تعطيل الخدمة. ومن الأمثلة ما قامت به مجموعة ألمانية (Adolf & Hitler. Com) بإمطار مجموعة من الطلبة اليهود بألمانيا بحوالي (17) ألف رسالة تحوي تهديدات بإعادة المحارق (Holocaust)، ولقد هدد المرسل بأنه سيحتفل بيوم (1938/11/9) اليوم الذي سمي ليلة كسر الزجاج (Night of Broken Glass) عندما بدأت ألمانيا النازية بمهاجمة اليهود فيها. ولم تستطع الشرطة الألمانية التحقيق في ذلك لأن البريد أرسل من خادم حاسب في الولايات المتحدة (Borchgrave et. al., 2000)

9- **الإعلان** (Advertising)

تستخدم الإعلانات في إدارة الإدراك للمنافسة في جذب انتباه المشترين، وليس جيمع أنواع الإعلانات هي حرب معلومات وإنما تصبح حرب معلومات عندما تستخدم المعلومات في تضليل الناس في شراء منتجات غير مرغوب فيها أو خاطئة من خلال الإقبال أو البريد الإلكتروني غير الموثوق فيه.

10- **الاحتيال المالي** (Scams)

تكثر وسائل الاحتيال المالي سواء كان ذلك بالهاتف أو بالبريد التجاري أو بالصحف. وغالباً ما يقدم المحتال وعوداً بالفوز بمبالغ كبيرة من المال من خلال جائزة أو يا نصيب... إلخ. ومثال على قصص الاحتيال ما تعرضت له هيلدا حنا، حيث تم الاتصال بها من كندا، وأُعلمت إنها فازت بمبلغ (945.000) دولار من المقامرة والمطلوب منها إرسال مبلغ (19.000) دولار لتغطية رسوم الضرائب والاتعاب في كندا، أرسلت المال ولم تحصل على شيء، بعد شهرين تم الاتصال بها مرة أخرى وطلب منها ارسال مبلغ (15.000) لتغطية الرسوم، ولقد دفعت ضحية احتيال أخرى مبلغ (4.000) دولار حيث وعدت أن تربح (128.000) دولار. وتبرر ذلك بقولها إن عمرها (71) سنة وأنها تثق بالناس (Schneider, 1997). تقدر خسارة الولايات المتحدة من الاحتيال المالي من خلال الاتصالات (40) مليار دولار سنوياً.

ولقد شاع استخدام اسماء أبناء لزعماء من دول أفريقية بأن لديهم ثروة تقدر بملايين الدولارات ويجدون صعوبة في اخراجها أو استثمارها ويرغبون «بك» في مشاركتهم ويطلبون رقم حسابك وأن المحامي سيتصل بكم . .الخ. وهذه أمثلة أخرى من الاحتيال المالي.

11ـ بريد القمامة الإلكتروني (Spam Wars)

يعني بريد القامة، البريد الإلكتروني الذي يرسل للأفراد لاقناعهم بسلعة معينة أو اشتراك ما، أو أحياناً إرسال كميات كبيرة من الرسائل أو ذات حجم كبير للحرمان من الخدمة. إن عملية قراءة وحذف (مسح) الرسائل عملية فيها إضاعة للوقت، والذين يقرأون بريدهم باستمرار يجدون فيها إضاعة وقت إن حملوا (Download) هذه الرسائل. ولقد أخذ الاسم (Spam) من مسرح (Monty Python) حيث تقدم المضيفات عشاء الاختيارات هي (Spam, Spam, Spam and Spam)، (Reuterss, 1998). إن غالبية هذا النوع من البريد هو الاحتيال المالي والبعض الآخر لزيارة مواقع الرذيلة وحوالي (5%) فقط هي دعايات لأعمال قانونية.

12ـ الرقابة (Censorship)

يمكن النظر للرقابة الحكومية كفعل عدوان وكفعل دفاع في حرب المعلومات. وفي مجال حرب المعلومات الهجومية، فإن حرمان شرائح من المجتمع من الوصول إلى المعلومات يعد عدواناً معلوماتياً، وكذلك حرمان وسائل الإعلام من الوصول للمعلومات، وحظر الخطابات. أما في مجال حرب المعلومات الدفاعية، فإن الهدف هو حماية المجتمع من المواد التي تؤذي الحكومة أو الثقافة، إنها تمنع وصول الرسائل النفسة التي تهدف للتأثير على المجتمع من مجتمع آخر، أو من الخصم.

إلا أن الرقابة الحكومية قد أصبحت غير ممكنة كما كانت في السابق، وكما يقول جيمس آدمز رئيس مجلس الـ (Sundy Times of London) إن أيام الرقابة الفعالة المصممة للتأثير على الرأي العام لدعم سياسات الحكومة قد ولت، ولم يعد بمقدور الحكومات ضبط تدفق المعلومات . . . والذي يمكن عمله ليس الضبط بالمنع والقمع للأخبار ولكن الضبط في انتقاء المعلومات (Adams, 1996).

وعلى الرغم من ذلك لا زالت الحكومات تراقب الإعلام، أظهرت دراسة مؤسسة بيت الحرية (Freedom House) أنه من بين (186) دولة هناك (67) دولة فيها حرية إعلام (Associated Press, 1998). فبعض الدول تراقب التلفون، والتلفزيون، والإذاعة، والفاكس، والفضائيات الداخلية والخارجية. وكذلك هناك دول قلقة من دخول الإنترنت. هذا بالإضافة إلى مراقبة المواقع على الإنترنت وحجب بعضها لأسباب متنوعة دينية، أو سياسية. ففي فينمار (بورما) يحبس لمدة (15) سنة أي شخص يستخدم أو يمتلك أو يستورد جهاز مودم أو فاكس دون موافقة مسبقة من الحكومة. ونفس العقوبة تطبق على أي شخص يقوم بوصل جهاز الحاسب مع أي شبكة معلومات دون موافقة (Financial Times, 1996).

13ـ التلوث الثقافي

يعني التلوث الثقافي أضعاف الأعراف أو تصارعها أو غيابها من خلال تقديم معلومات غير صحيحة ومشكلة. وتهدف هذه الاساليب إلى التأثير على المعتقدات وتحويلها باتجاهات معنية.

ويشمل مجموعة من التهديدات التي يتم نشرها من خلال العمل على شبكات الحاسب وخاصة الإنترنت ومنها :

أ ـ التهديد للمعتقدات: وتتمثل هذه المواد في صفحات على الشبكة تحتوي على أفكار تشكيكية ومتطرفة، تمس الدين، وتمثل هذه المواقع مواقع جذب للمراهقين والشباب حيث تمتاز مرحلة المراهقة والشباب بعدم الاستقرار النفسي والاجتماعي مما يجعل الأفراد أكثر عرضة للتغير واسهل في تغير معتقداتهم مما يشكل خطراً اجتماعياً عاماً.

ب ـ التهديد الإخلاقي: تجمع المجتمعات على قواعد أخلاقية ذات طبيعة إنسانية عامة، وهذه النظم الإخلاقية تشكل دعامة النظم الاجتماعية، إلا إنها تتفاوت من مجتمع لآخر، وفي الإنترنت الكثير من المواقف وخاصة الجنسية منها والتي تشكل مادة جاذبة للمراهقين والكبار مما يؤدي إلى انغماسهم في خيالات وصرف اهتمامهم وتخريب شخصياتهم في مرحلة مبكرة يضعف بموجبها التحصين الاجتماعي والأخلاقي لديهم، وهذا التهديد للنظام

الأخلاقي ينعكس بتهديد النظم الاجتماعية الأخرى. وتسهم هذه المواد في تدمير القيم نظراً لما تحوية من آلاف الصور الجنسية الفاضحة والأفلام الإباحية (الخطيب، 1997).

ج ـ التهديد الأمني : تشمل الإنترنت وبعض الشبكات الأخرى، معلومات هامة كافية لاستخدامها من قبل الهواة والعابثين في إنتاج وتركيب القنابل أو المواد التي يمكن أن تستخدم في الإرهاب أو الأعمال التخريبية، مما يشكل تهديداً لأمن المجتمع عامة. ولقد قدمت معلومات في الكونجرس الأمريكي تبين أن الشخص يمكن أن يكون قنبلة دون أي علم سابق وذلك باعتماده على المعلومات المنشورة على الإنترنت (البداينة، 1998). وقد أبدت الدول الصناعية الكبرى (G7) وروسيا مخاوفها في اجتماع باريس (1996) من أن التنظيمات الإرهابية يمكن أن تستخدم شبكة الإنترنت، وتوظيفها لخدمة أهدافها، وخاصة بعد حادث تفجير (أوكلاهوما سيتي) في العام 1995م، (الشهاوي، 1998).

14ـ **التوهج** (Flaming)

يعني التوهج إرسال رسالة أو رسائل غليظة ومنتهكة حرمة القوانين وخصوصية الأفراد إلى فرد أو مجموعة أفراد أو مجموعات أو إلى المجتمع كله. وعادة ما يشمل التوهج الإهانة والوقاحة كأسلوب في تحقير الآخرين، وهي طريقة لا تتماشى مع ما ينادى به من آداب التعامل على الشبكة (Etiquette). وينصح بأن لا يرد مثل هذه الرسائل فوراً، بل يؤجل الرد إلى اليوم التالي، ويمكن استخدام مكالمة هاتفية أو محادثة شخصية (روسينبرج، 2000).

الفصل التاسع

الداخليون

مقدمـة

يُعد الداخليون (الموظفون وخاصة المطلعون على الأسرار) سواء من العمال أو الموظفين أو أصحاب المناصب المؤتمنون في المؤسسة التحدي الكبير على مصادر المعلومات، ومن المحتمل أن يستغلوا مصادر المعلومات للكسب الشخصي أو لتخريب أنظمة الحاسب، وذلك من أجل الانتقام كما يمكن لهم أن يكشفوا الأسرار ولو بصفة غير متعمدة من خلال التعامل مع المقاولين والشركاء والزبائن والزوار والطالبين للمعلومات من خارج المؤسسة. ويغطي هذا الفصل عمليات حرب المعلومات الهجومية من قبل الدخلاء (العاملين) في المؤسسات الذين لديهم فرص الحصول على مصادر المعلومات . وتشمل هذه العمليات على الوثائق والمطبوعات وملفات الكمبيوتر ومناطق المؤسسة الفعلية التي تتعلق بشؤون الموظفين .

ويتناول هذا الفصل مواضيع تتعلق بالحصول على المعلومات من قبل الدخلاء (العاملين في المؤسسة) ويتضمن ذلك العلاقات التجارية والزيارات والطلبات والخونة والجواسيس، كما يتناول الاحتيال، والاختلاس، وأعمال التخريب من قبل الدخلاء ضد مصادر المعلومات.

1ـ الخونه والجواسيس.

يتناول موضوع الخونة والجواسيس الطرق والاساليب التي يستخدمها هؤلاء الأفراد في التعامل مع المعلومات، وتقسم هذه القضايا إلى أربعة أصناف هي: جاسوسية الدولة والعسكرية، التجسس الاقتصادي، التجسس المشترك والاتفاقات السرية. كما يصف هذا الفصل الطرق والأهداف وتأثير العمليات .

أ ـ جاسوسية الدولة والجاسوسية العسكرية: يشير هذا الصنف إلى العمليات من قبل الوكالات الأجنبية وذلك بغرض الحصول على أسرار الدولة العسكرية ضد الدول الأخرى، وذلك باستغلال خدمات الخونة والدخلاء والرجال المكلفين بهذه العملية (العملاء) والجواسيس الذين يعملون لحساب الدول المرسل إليها وذلك لأجل المراقبة، وفي الحقيقة هؤلاء بعض العملاء يعملون لحساب الطرفين وعلى سبيل المثال

يوجد نفي قضية (جون ايه والكر John A - Walker)، وهو رجلاً ذا سمعة عاليه وضابطاً متقاعداً في القوة البحرية الامريكية وكاتب اتصالات سابقاً وقد باع والكر الرموز السرية والوثائق إلى الاتحاد السوفيتي والتي تغطي الفترة من 1967م حتى اعتقاله في 1985م لقد تمكن الاتحاد السوفيتي بهذه الرموز أن يقرأ حوالي مليون رسالة سرية، كما منح واكر الاتحاد السوفيتي الخطط البحرية في المستقبل ومواقع السفن وبيانات من الأسلحة والتكتيكات البحرية وعمليات مكافحة الاستخبارات وخطط الطوارئ في حالة الحرب النووية. وقد حكم على واكر بالسجن مدى الحياة مع أخيه أرثر (Arthur) الضابط السابق في القوة البحرية وصديقه جي ـ إية ـ وايت ـ ورث (J.A. White worth) الخبير في أمور الإتصالات البحريه، فكلاهما كان يعمل في تزويد الوثائق السرية، كما حكم على مايكل (Michael) خمسة وعشرين عاماً عقوبة بالسجن وهو ابن واكر وكان يزود الوثائق السرية لأبيه، يذكر رونالدكيسلر (Ronald Kessler) في كتابه « جاسوس ضد جاسوس » قصة كارل كوشر (Karl - Koecher) وهو قادم إلى الولايات المتحدة سنة (1965) بعد رجوعه من شيكوسلوفاكيا (Czeckoslovakia) وبدأ يعمل مع السي ـ أي ـ ايه (CIA) كمترجم ومحلل وترك هذا العمل في سنة (1977) ولكن استمرت العلاقات على صورة الموظف المقاول وفي النهاية اعتقلته هيئة التحقيقات الفدرالية (FBI) وزوجته سنة (1984) وطوال فترة إقامته في الولايات المتحدة خلال عشرين سنة كان يعمل جاسوساً سوفيتياً للمخابرات السوفيتية (KBG) ودائرة المخابرات التشيكوسلوفاكية وقد أعطى تفصيلات خطيرة عن عمليات سرية للمخابرات الأمريكية (CIA) ووثائق سرية وقوائم وصور عاملين في (CIA) وأسماء أشخاص قد يمكنهم التعاون مع السوفيت .

كما يوجد للولايات المتحدة جواسيس من الأجانب يشتغلون تحت إدارة (CIA) وتسجل قضية في «نيويورك تايمز New York Times) عن شخص تايواني الجنسية عين في سنة 1960 من قبل (CIA) باسم جانج هين آي (Chang Hsein. I)، وقد دربته (CIA) لمدة عقدين كاملين حتى أصبح المدير المساعد لمعهد البحوث النووية ولقد أقنعت أمريكا الحكومة التايوانية أن تترك عملها على البرامج النووية وذلك بجهود (جانج. هين. أي) (Chang - Hein I.)، حين سلم إلى (CIA) (سي أي ايه) الوثائق المهربة ومما يذكر أن الصين قد هددت بالهجوم على تايوان إذا امتلكت القنبلة النووية في هذا الوقت قدمت الحكومة الأمريكية الدلائل القاطعة على ذلك بناء على

الوثائق التي سلمت لهم من قبل (جانج هين آي)، وهذا أصبح سبباً في وقف برنامجها النووي التايواني ومما لاشك فيه أن هذه القصة تبين مدى الحاجة إلى الجواسيس، وبناءً على هذه القصة قال بعض الضباط السابقين إن حصول جانج على وثائق مسروقة قد أدى إلى توقف البرنامج الذي لم يكن هناك امكانية لإيقافه من قبل المراقبة الدولية في خلال فترة عشرين عاماً .

ب ـ **التجسس الإلكتروني**: استقال أحد الموظفين الصينين من شركة Ellery) (Systems حاملاً معه برمجيات ورموزاً أساسية (Source Codes) تقدر بـ (950) ألف دولار يمكن أن تؤدي عند إنتاجها إلى مليارات الدولارات، وكنتيجة لذلك فقد سرحت الشركة كل موظفيها وأعلنت إفلاسها. ولم يتم إدانة الموظف على الرغم من الإثباتات التي لدى (FBI). وبسبب الثغرات وضعف التشريعات المتعلقة بالتجسس الاقتصادي وبسبب حالة شركة أليري للنظم تم تعديل قانون التجسس الاقتصادي عام (Shaw, 1996) وخلال (20) عاماً تم اعتقال وإدانة أمريكان يتجسسون لحساب كوريا الشمالية، وتايوان، والفلبين، وإسرائيل، والسعودية، والعراق، والأردن، وجنوب أفريقيا . . . إلخ. بالإضافة إلى روسيا والصين Wood and) . Wiskoff, 1992)

ومواضيع التجسس العسكري تشمل البحث عن أسرار عسكرية، ونظم دفاعية عسكرية، ومعلومات سرية وتقنيات. إن خطورة التجسس في هذه المجالات هو زيادة التنافس الدولي وعولمة الاقتصاد واعتماد الشؤون العسكرية والاقتصادية وفرص العمل على هذه الأسس، كما إنها هي التي تضمن التفوق الاقتصادي والعسكري للدول الصناعية. خاصة إذا علمنا أن الولايات المتحدة تنفق سنوياً حوالي (300) مليار على البحوث الأساسية وبالتالي فإن التجسس التقني والاقتصادي هو استثمار غير شرعي لهذا الاستثمار (Sowboda, 1996) .

ويشكل النقل غير القانوني للتقنية (Illegal Technology Transfer). من الدول الصناعية إلى الدول المنافسة والنامية مشكلة بالنسبة للدول الصناعية من الناحية الأمنية، تنظر الدول الصناعية وخاصة الولايات المتحدة الأمريكية إلى أن وصول تقنيات وخاصة ذات التطبيقات العسكرية إلى الدول المنافسة (روسيا، وكوريا الشمالية، والصين، والعراق) وحتى الأوروبية مهدداً أمنياً لهذا القطاع. وينظر إلى

هذا الموضوع من جانبين، الجانب الأول الكلفة المادية للتطور التقني، والجانب الآخر المردود المادي الذي ينجم عن المبيعات خاصة إذا تم نقل هذه التقنيات بسعر رخيص (مثل بيع الأقراص المدمجة للبرمجيات الخاصة بالحاسب). كما أن بعض هذه التقنيات يمثل سراً عسكرياً أو تقنياً، فمثلاً في تقرير للـ(FBI) بين أن الـ(KGB) قد حصلت على(12000ـ13000) عينة من المعدات من الغرب كل سنة في الفترة (85ـ86، 88ـ1989) وغالبية هذه المواد تم الحصول عليها من الولايات المتحدة.

وفي دراسة على النقل غير القانوني للتقنية في الولايات المتحدة خلال مدة (12) سنة تبين أنه نقلت تقنيات غير قانونية إلى (56) دولة وكانت هذه المعدات موزعة على النحو التالي : (36%) استخدام مزدوج (حاسبات ذات سرعة فائقة، مرآة ليزر)، و(31%) مكونات أسلحة (معدات رادارات)، و(15%) أسلحة كاملة (مثل صواريخ تاو)، و(13%) معدات عسكرية (رؤية ليلية)، و(3%) معدات تجارية (محركات طائرات). ويتم نقل هذه المواد عادة إلى دولة صديقة للولايات المتحدة ومنها إلى الدولة المعنية، وغالبية هذه المواد شحنت أولاً إلى دول مثل ألمانيا، وبريطانيا .(Garthoff, 1996)

ج ـ **التجسس الإقتصادي**(Economic Espionage)، يستهدف التجسس الاقتصادي بشكل خاص المؤسسات والشركات، والأفراد، ويشمل: الحصول على معلومات حساسة بطرق غير قانونية تتعلق بالمال، والتجارة، أو السياسة الاقتصادية، ومعلومات اقتصادية عن السلع والمنتوجات، وعن التقنيات الحساسة، أو الحصول على معلومات اقتصادية حساسة تتعلق بالقرارات المرتبطة برسم السياسات الاقتصادية للدولة. ويشير هذا إلى العمليات من قبل الحكومات لاكتساب الأسرار الاقتصاديه لأي بلد اجنبي ويضمن هذا الحصول على معلومات حول سياسات التجارة أو الأسرار التجارية لبعض شركات البلد الأجنبي، إذ أن هذه المعلومات تسلم إلى شركائهم لأجل المنافسة، فمثلاً دور المخابرات الأمريكية في حرمان الفرنسيين من توقيع عقود تجارية كبيرة مع بعض دول الخليج العربية.

وقد يغري العاملين أحيانا بوعد الحب او الرفقة مقابل الحصول على أسرار التجاره ويذكر ايرا وينكلر (Ira Winkler) في كتابه "التجسس المؤسسي(Corporate Espionage)، عن قصة جاسوس ألماني يسمى كارل هينرش ستولز (Karl Heinrich

(Stohlze) بعد وصوله إلى بوستن سنه (1989) أقام علاقة مع المرأة الوحيدة التي كانت تعمل لشركة علم التقنيات الحيوية (Biotechnology) وتم استغلال العلاقة معها بطريقة خادعة وقال لها أنه سيتجه إلى ألمانيا إذا فشل في الحصول على بعض الوثائق وخوفاً من فقدان الرفقة معه بدأت هي بتزويده بالوثائق المطلوبة وبعض أسرار الشركة وهذا ضمن الطرق البحثية والمعلوماتية الخاصة به (D.N.A) عن وضع مشاريع الشركة وهذا مثال لاستغلال العلاقات الجنسية في الحصول على المعلومات .

ج ـ التجسس المؤسسي: قدر ايرا وينكلر في كتابه التجسس المؤسسي (Corporate Espionage) أن هناك عدة مئات من الدخلاء المحترفين (الأذكياء) الذين يمكن أن يكتشفوا الثغرات الأمنية في نظم المعلومات، وخمسة أضعاف هذا الرقم من المبرمجين القادرين على استغلال تلك المعرفة. ويتناول في هذا الكتاب العديد من حالات التجسس مثل حالة انتل، وبوينج، وغيرها (Winkler, 1997).

يشير التجسس المؤسسي، أو التجسس الصناعي إلى العمليات التي تأخذها شركة واحدة ضد شركة أخرى وذلك لحساب فائدة المنافسة في الأسواق المحلية والعالمية، ومن المحتمل أن يكون المنافس أجنبيا أو وطنياً، وعلى سبيل المثال هناك قضية ذات شهرة عالمية وهي أن (جنرل موتور) اتهمت رئيس مشترياتها السابق لوبز (Lopez)، وسبعة من الموظفين الآخرين بأنهم أخذوا (10000) وثيقة وأقراص حاسبة معهم، عندما التحقوا بفولكس واجن (Volks Wagen)، وقد حصل هذا الحدث قبل الالتحاق إلى فولكس واجن (Volks Wagen)، وهي معلومات عن بعض أقسام (جنرل موتورز) حول العالم. وقد وجد أربعة صناديق مملوءة بالوثائق داخل شقته في وسبادين (Weisbaden) في ألمانيا، وتضمنت هذه الصناديق تفصيلات عن أسرار نموذج سيارة جديدة واستراتيجيات المبيعات المستقبلية وقوائم الشراء. وبناءً على هذا رفعت (جنرل موتورز) دعوى قانونية ضد الأشخاص المذكورين في سنه (1996)، وذكرت في هذه الدعوى أن شركة (جنرال موتورز) قد خسرت مائه مليون دولار أمريكي نتيجة احتيال الاشخاص المذكورين.

د ـ جمع المعلومات الخاصة. يقوم بعض العاملين في المؤسسات بجمع بيانات خاصة خزنت على الكمبيوترات الموجودة لدى مؤسساتهم، ففي سنة 1996قام بعض العمال ببيع بعض البيانات المفصلة عن (11000) شخص من مكتب إدارة التكافل

الاجتماعي في بروكلين. وفي فلوريدا أخذت الأسماء عن مرض الإيدز من الكمبيوتر Pinellas County (مقاطعة بيانلس)، وأرسلت إلى (St. Peterburg Times) سينت بيتربيرج تايمز للنشر في 18 سبتمبر سنة (1996)، ويمكن بيع معلومات عن الزبائن، وهذا رائج الآن على الإنترنت تشمل اهتمام الناس مما يعني أن الشركات المتنافسة يمكن أن تصنف هذه المعلومات وفق اهتمامات الأفراد، وتسهل عملية الوصول إلى هؤلاء الأفراد كسوق لمنتجاتهم وإرسال الدعايات، والعروض لهم من خلال البريد الإلكتروني.

2ـ علاقات العمل

من الممكن أن تُكتسب أسرار التجارة باستغلال علاقات العمل ويتضمن ذلك علاقات مع المقاولين والزبائن والشركاء في قضية واحدة مستمرة قد أخذ مشرف الشركة فرصة الدخول لكل مكتب في مركز البحوث بي. بي.جي (PPG). وسرق القوائم الخاصة بالزبائن، وصور الرسم والمخططات، والقواعد السرية والوصفات الإنتاجية، وشرائط الفيديو، وقد أرسل باتريك ورتنج (Patric Worthing) عرضاً إلى أوون كورنج (Owen Coroning) لبيع أسرار بي. بي جي (PPG) مقابل ألف دولار أمريكي ولكن أوون (OWEN) رفض العرض ـ أوون كان منافس بي ـ بي ـ جي (PPG). ومن الجدير بالذكر بأنه قد حدث نفس الأمر قبل سنتين وفي ذلك الوقت رفض بي ـ بي ـ جي(PPG) استلام الأشياء المسروقة من أوون (OWEN) قبض مكتب التحقيقات الفدرالي (F.B.I) على جواسيس كلتا الحالتين وقد أدين ورتنج وحكم بالسجن خمس سنوات تحت قانون التجسس الاقتصادي.

3ـ الزيارات والطلبات

يمكن الحصول على أسرار المؤسسة التجارية عن طريق الزيارات أو الطلبات في هذه الأحوال ، قد يقدم موظفو المؤسسة المعلومات الهامة عن غير عمد للزوار الذين يستعملون أساليب الهندسة الاجتماعية للحصول على المعلومات من الموظفين إما شخصياً أو عن طريق الهاتف. ويذكر وينكلر (Winkler) في كتابه «التجسس المؤسسي» (Corporate Espionage) بعض الوقائع التي تبين الأمثلة عن استعمال مهارات الهندسة الاجتماعية ويقول بأن القوة الاقتصادية الأمريكية تأسست جزئياً على

مهارات التجسس من قبل رجال الأعمال في القرن التاسع عشر. ومن الأمثلة واقعة فرنسيس كابوت لوويل (Francis Cabot Lowell) وهو من سكان برستن ومتخرج من جامعة هارفرد (Harvard) وكان رجلاً غنياً جدا ـ سافر إلى أدنبرج (Edinburg) مع زوجته وأطفاله الصغار وسكن هناك . واخبر الجيران بأنه في اسكتلندا (Scotland) لأسباب صحية ـ لكنه في الحقيقة كانت له أهداف أخرى وهو الحصول على أسرار صناعة النسيج المزدهر في بريطانيا وقام برحلات عديده في الريف وزار بعض المدن مثل لينكشاير Lancshire ودربي شاير (Derbyshire) التي تتواجد بها المصانع الحديثة وكانت هذه المصانع ناجحه وتجذب الثروات الضخمة، وبعد أن حقق لوويل (Lowell) أهدافه عاد إلى وطنه في أمريكا ووضع معرفته وخططه لحركة صناعة النسيج في أمريكا .

يوجد لدى بعض الشركات وحدات تسمى الاستخبارات المنافسة ـ وهم يقومون بجمع المعلومات المطلوبة ضد المنافسين عن طريق الإجراءات القانونية ـ ومن الأمثلة على ذلك لويس جيرشترنر (Louis Gerstner) عندما أصبح الرئيس التنفيذي، عين عدة فرق للجاسوسية في (اي ـ بي ـ ايم I.B.M) يتضمن (نظام الجاسوسيه) وهو نطام شامل عن الجاسوسية الإنسانيه وكانت تستهدف المستشارين، والموردين ، والزبائن أو الموظفين للمنافسين، والمعلومات التي تم الحصول عليها عن طريق هذه الفرق وضعت في قاعدة بيانات مركزيه تصل إلى450 من الرؤساء التنفيذيين .

4ـ الاحتيال والاختلاس

أدى اتساع استخدام الشبكات العالمية، وخاصة الإنترنت إلى زيادة كبيرة في التجارة الإلكترونية عبر الشبكات، وأدى هذا الاتساع إلى زيادة جرائم النصب، والاحتيال المالي، وتطورت أساليب النصب والاحتيال بالطريقة ذاتها التي تطورت فيها الشبكات.

ومن أكثر صور النصب والاحتيال التي تتم عبر شبكة الإنترنت نشر وإعلان ووضع مواقع على الشبكة تتعلق بتجارة سلع، أو تقديم خدمات وهمية وغير موجودة حيث تتصيد هذه المواقع المبالغ المالية للمشترين عبر الشبكة، وعن طريق وسائل الدفع

المختلفة، وخاصة بطاقات الائتمان (البحر، 1999). وقد يستغل موظفو البنوك، والشركات الاخرى نظام معلومات الشركة للكسب المالي عن طريق عمل صفقات زائفة والعبث بأنظمة المعلومات .

5ـ الصفقات المصطنعه

تمثل التعاملات الزائفة شكلاً من أشكال الاحتيال، وتمثل التحدي الأكبر إلى الأنظمة المالية، وتكثر الصفقات المصطنعة من خلال الداخليين (العاملين في المؤسسة) فعندهم امكانية الوصول إلى الانظمه ـ فمثلاً قام المحاسب في شركة بنكرتن لأمن وخدمات التحقيق (Pinkerton Security and Investigation Services) بسرقة أكثر من مليون دولار من وكالة البحث الجنائي (Detective Agency) عن طريق نقل المبلغ من حساب بنك الوكالة إلى حسابات الشركات الزائفة.

6ـ تعديل البيانات

وهذا شكل من أشكال الاحتيال والتزوير، يشير هذا إلى تعديل البيانات الموجوده ويتضمن الوثائق، والسجلات، والصور، والبرامج. تعديل البيانات يؤدى إلى ضياع سلامة البيانات ولكن المجرمين ربما يكسبون مادياً ، اما المالك فهو يعاني خسائر كبيرة. وهذا ما قد يحصل في سجلات الضرائب بتعديلها لكي تبدو مدفوعة، أو أي سجلات أخرى مشابهة.

والعبث بالبيانات قد يؤدي إلى نتائج مهمة عندما يتعلق النظام بحياة الإنسان كالرعاية الصحية. ففي بريطانيا أدين الممرض بالعبث بالسجلات بعد دخوله للنظام الكمبيوتري في المستشفى، وذلك بتعديل في وصفات الأدوية للعلاج من مثل أن يُعطى علاج أمراض القلب وضغط الدم العالي إلى طفل عمره 9 سنوات مصاب بالإلتهاب السحائي.

7 ـ التخريب الداخلي

للعاملين في المؤسسة فرص لأعمال تخريبية على مصادر المعلومات إما باستعمال الأسلحة فعلياً أو بتدمير برامج الكمبيوتر ـ قد تسيء هذه العلميات نزاهه المصادر، كما تجعل هذه المصادر غير متوفرة إلى مالك المؤسسة التجارية في بعض القضايا، وقد تدمر مصادر المعلومات كلها مما يؤدى إلى االإضرار بسمعة الشركة، ويؤدي إلى فقدان الزبائن والمبيعات.

وفي الدراسة المسحية التي يقوم بها (AAB5, 1989) فقد تبين أن أكثر التهديدات الداخلية من المستخدمين غير القانونيين وبنسبة (79%)، يليها الموظفون المصرح لهم حيث بلغت نسبتهم (78%)، ثم الموظفون السابقون بنسبة (75%)، وموظفو العقود بنسبة (75%).

8ـ الهجمات الفعلية: هي الهجمات الفعلية ضد أي عنصر من نظام المعلومات مثل الكمبيوتر، والطابعات، وأدوات التخزين، وأنظمة الاتصالات، والمواد المطبوعة أو الموظفين ـ كما يمكن للمهاجمين أن يستعملوا الأسلحة من السكاكين إلى المتفجرات القوية. وقد يستخدم العنف بين الأفراد أو التصفيات الجسدية، كما يستخدم التعدي على المعلومات كالوثائق والأقراص.

9 ـ الهجمات البرامجية: الهجوم على البرامج هو الفعل الذي يؤدي إلى تخريب أو تدمير بيانات خزنت على الكمبيوترات وبسبب ذلك يمكن توقيف العمليات التجارية العادية وإلحاق الخسائر المالية بالأطراف الأخرى، ويمكن تدمير هذه البيانات عن طريق القنبلة المنطقية ـ هذا البرنامج يبقى نائماً حتى يحدث الحدث ـ هو ينفذ حينئذ ـ وإذا حدد لذلك وقت أو تاريخ يسمى البرنامج «القنبلة الموقوتة».

يوجد هناك أمثلة عديدة تمثل ظاهرة القنابل المنطقية. في معظم الأحوال يحفظ القنابل المنطقية موظفون ساخطون على أنظمة الشركة عند استلام إنذار لإنهاء العمل في الشركة ـ إن الرمز السيء يدخل وينفذ بعد بضعة أيام. دونالد جين برلين محلل أنظمة الأمن في شركة التأمين بتكساس، حذف (168000) سجل للبيع بعد أن أعلن بترك العمل بالشركة .

10ـ انتحال صفة الآخرين (Masquerading): للحصول على دخول إلى النظام في الحاسب، ويمكن أن يحصل هذا التعدي من خلال أشخاص، أو عن بعد، ويجب أن تمنع إجراءات السلامة انتحال صفة الآخرين بقصد الدخول إلى نظام الحاسب، ومن أنواع هذه التعديات الدخول إلى نظام حماية التشغيل (Operations Security). وهناك انتحال فيزيقي، أو الكتروني للآخرين. فمن الممكن أن يستخدم المجرم هوية مزورة للدخول إلى المناطق المحظورة، أو الدخول إلى مبنى مركز المعلومات، أو الحاسب. ويمكن استخدام أسلوب التظاهر (Piggybacking)، وهو أن يحمل الفرد معدات حاسب ويظهر بمظهر الذي ينتمي للمكان لكي يتمكن من دخول المبنى،

ويمكن استخدام الانتحال الإلكتروني من خلال استخدام كلمة المرور (Password)، أو الدخول (Logon In) أو الرقم الشخصي (Personal Identification Number [PIN])، أو رمز التلفون (الصوت) . . . إلخ.، ولفهم كيف تتم عمليات الانتحال، لابد من فهم كيفية التعرف على الهوية من قبل نظام الحاسب.

الهوية طريقة تخبر النظام فيها من أنت ؟ مثل أن تدخل رقم الحاسب، أو كلمة المرور . . .إلخ، وهناك ثلاث طرق لإثبات من أنت وهي :

1ـ شيء تعرفه، كرقم الهوية، أو كلمة المرور.

2ـ شيء تملكه، مثل مفتاح المبنى، أو البطاقة الذكية.

3ـ شيء منك، أوتفعله، مثل الصفات الفسيولوجية، مثل بصمة اليد، أو بصمة الصوت، أو توقيعك.

ولسوء الحظ فإن من الشائع لدى مجرمي الحاسبات سرقة، أو تخمين الأسماء، وكلمات المرور، وعندما ينتحل شخص شخصيتك، فإنه يستطيع أن يفعل ما يمكن أن تفعله أنت. ويمكن للمحتال المنتحل لصفة الآخرين أن يؤذي صاحب النظام بإرسال رسائل سيئة باسمه، مثلاً، أو تدمير سمعته المالية، أو الشخصية، فمثلاً قد يرسل طالب رسالة باسم المدرس يقول فيها للطلاب بأن المدرس يعتذر عن تقديم الامتحان لأسباب عائلية مما يؤدي إلى غياب الطلبة عن الامتحانات.

الفصل العاشر

مُصادرة الاشارات

مقدمة

تتزاحم في بيئتنا الطبيعية الكثير من إشارات الطاقة، والإشارات المغناطيسية، هذه الإشارات هي التي تمكن من السمع والرؤية للمواد من حولنا. وبفعل هذه الإشارات يتمكن الطيارون من الطيران، وتوفر كافة الاتصالات (المكالمات الهاتفية، شبكات الحاسب، إشارات التلفزيون والراديو، الفاكس... إلخ) والإشارات الكهرومغناطيسية موجات تنتقل من خلال وسيط ـ الهواء، والماء، والنحاس، والألياف الضوئية ... إلخ. وأي إشارة (Signal) يمكن أن تصنف من خلال مدى التردد (الطول)، حيث كل تردد يعبر عنه بعدد من دوائر الموجات (التكرار) لكل ثانية. والتردد يمثل بالهيرتز (Hertz [Hz])، حيث كل ميقاهيرتز (1MHz) تساوي (1) مليون دائرة في الثانية. أما عرض الموجة فيشير إلى الفرق بين الترددات العليا والدنيا في الموجة. ويشكل هذا المدى من الترددات ما يسمى بالمجال الكهرومغناطيسي، والذي يشمل (الترددات الدنيا والعليا)، الترددات المنخفضة (ELF)، أو ما تعرف (Extra low frequency)، وأمثلة استخدام هذه الموجات استخدامها في خطوط الهاتف، ومجال الراديو، والأشعة دون الحمراء (X-rays)، وأشعة جاما، وأشعة كومك (Comic). ويتراوح مجال الراديو بين الموجات المنخفضة والعالية جداً، وتشمل (أف أم FM)، و(اي أم AM)، والموجات القصيرة، والتلفزيون، والتلفون اللاسلكي، والبيجر (النداء) والجوال (Cellular Phone). ولكل مدى من هذه الموجات (Denning, 2000 b).

ويستخدم مصطلح «استخبارات الإشارات» (Signals Intelligence)، أو المختصرة بـ(Sigint) للإشارة للعمليات المتفرعة التي تشمل اعتراض وتحليل الإشارات عبر المجال الكهرومغناطيسي، وبعد عملية الاعتراض فإنه يتم حل رموز وحل تشفير وتحويل وتلخيص وتحليل الإشارات لإنتاج المادة الاستخبارية.

اعتراض الاتصالات (Intercepting Communications).

هناك الكثير من الدول الصديقة والعدوة التي تعترض الاتصالات للحصول على معلومات استخباراتية في مجال السياسة والاقتصاد والتجسس العسكري. ان غالبية الاتصالات والفاكسات ترسل عن طريق الفضاء من خلال الموجات اللاسلكية وهذه الموجات غالباً ما تُعترضَ.

إن غالبية الأدوات التقنية مثل التلفون والنقال واللاسلكي والبريد الإلكتروني والبريد الصوتي وآلة تسجيل المكالمات يمكن أن تستغل بطرق متنوعة. وإذا كان ما تكتبه أو تقوله أو ترسله يسبب الثراء أو الفائدة أو التأثير فانك هدف للاستغلال من خلال اعتراض ما تكتبه أو ترسله. ومن المواضيع التي تعد مكان اهتمام للاعتراض قوائم العملاء، وخطط التسويق، والبيانات المالية، والمفاوضات التعاقدية، والبحث والتطوير، وتقنية الانتاج.

وهناك صعوبة في معرفة إن كانت اتصالات معينة مراقبة، أو إنها اعترضت. وعامة هناك طريقتان لحماية اعتراض المكالمات الهاتفية والفاكسات:

1ـ لا تناقش أو تتحدث عن معلومات حساسة على الهاتف، أو ترسلها على الفاكس.

2ـ إذا كان لابد من استخدام الهاتف، أو الفاكس فشفر جميع الاتصالات الحساسة.

ولخفض فرص اعتراض مكالماتك وفاكساتك لا تسخدم جملاً أو كلمات تجعلك على قائمة المستهدفين من قبل أجهزة الاستخبارات مثل اسم المنظمة، المنتج، وأسماء الأشخاص . . . إلخ.

1- **التلفون** (Telephone).

يعد الهاتف بكافة أنواعه من متطلبات الحياة اليومية، ولكن الناس الذين يستخدمون الهواتف مسؤولون عن تسرب المعلومات الحساسة التي يفترض أن يحموها. ويمكن أن يشكل الهاتف خطراً على الإنسان بطريقتين:

1ـ اعتراض المحادثات الهاتفية والفاكسات في أي مكان وفي لحظة يتبين المرسل والمستقبل، وذلك من خلال الاتصالات الفضائية والمحطات الأرضية الفضائية، وتسجيل المكالمات (التجسس)، أو من خلال الهواتف النقالة واللاسلكية.

2ـ إن نظام الهاتف يمكن أن يتم انتقاؤه والولوج إليه، بحيث أن ميكرفون في يد الهاتف ينقل كل ما يجري في المنزل ويرسله من خلال خط الهاتف إلى المستقبل في مكان ما.

2- **خدمات الهاتف** (Phone Services) .

غالباً ما تقع خدمات الهاتف ضحية لقراصنة الحاسب والهاتف (Phreakers)، حيث يمكن أن تستخدم الأرقام الخاصة، أو الحكومية، أو الشركات لإجراء مكالمات، أو يمكن أن تحول المكالمات الواردة إلى أي مكان آخر، ويمكن في هذه الحالة استخدام المعلومات الواردة فيها خاصة إذا ربطت بآلة تسجيل تطلب معلومات عن المتصل، ووضع رسالة قصيرة، أو لمجرد معرفة المعلومات والمتصلين برقم ما من مثل رقم المحكمة أو الاستخبارات أو . . إلخ. وقد تستخدم للتحرش فمثلاً يمكن تحويل المكالمات لشخص ما إلى التلفونات الجنسية أو (1-800-Eat-S) .

لقد تمكن مراهق سويدي من نقل رموز (شيفرة) إحدى شركات الاتصال الأمريكية حيث تمكن من الاتصال مع أي شخص في الولايات المتحدة مجاناً، لقد شوش على اتصالات ولاية فلوريدا من خلال ربطها بـ (6) خطوط اتصال في آن واحد. وفي مدة ثلاثة أشهر تمكن من الاتصال في (911) رقم الشرطة في (11) موقعاً في شمال فلوريدا، ولقد أجرى (60.000) مكالمة بكلفة (250.000) دولار. وألقي القبض عليه وحكم في السويد ودفع غرامة (345) دولار (Denning, 2000 b) .

3- **التلفون (الجوال) والبيجر** (Cellular Phone) .

يوجد في الجوال ثلاث ثغرات أمنية (انكشافات) وهي على النحو التالي:

1ـ الانكشاف والتعرض إلى المراقبة للمكالمات والمحادثات خلال استخدام الهاتف.

2ـ انكشاف الهاتف نفسه بتحويله إلى ميكروفون لنقل ومراقبة المكالمات والمحادثات التي تتم حولها جهاز الهاتف.

3ـ تعرضه إلى التقليد (Cloning)، أو استخدام رقمك من قبل آخرين في اجراء مكالمات على حسابك.

والتلفون النقال (مرسل ـ مستقبل راديو) فالصوت يرسل من خلال الهواء على موجات الراديو. وموجات الراديو ليست مباشرة، إنها تتوزع في جميع الاتجاهات، ولذا فإن أي شخص يمكن أن يلتقطها باستخدام النوع المناسب من المعدات ويستمع

إليها. وهواة الراديو لهم مواقع يتبادلون فيها أرقام الجوالات ذات الاهتمام ويستمعون إليها.

ولأن الجوال يعمل من خلال مطابقة رقمين هما رقم هوية الجوال (MIN)، والرقم الإلكتروني المتسلسل (ESN) واللذين يعرفان بالزوج. وإذا ما تمت سرقة هذين الرقمين فإن ما يعرف بالجوالات المقلدة أو المقلدين يمكنهم برمجته في تلفون آخر ويصبح نسخة عن هاتفك الأصلي ويمكنهم عندها إجراء مكالمات من الهاتف (الجوال) المُقلد والكلفة على عنوانك.

من السهولة بمكان اعتراض المكالمات الصادرة، أو المرسلة إلى التلفونات الخلوية (Cellular)، خاصة قرب مراكز إرسال الميكروويف وأبراج الاستقبال. ويمكن استخدام أداة فاحصة (ماسحة) (Scanner) من مثل (Celltracker)، ويمكن اعتراض مكالمات الخلوي حيث يمكن إدخال رقم الهاتف من خلال لوحة المفاتيح. فمثلاً تستخدم شرطة نيويورك نظام يراقب (19) قناة اتصال، ومتابعة (3)محادثات متزامنة.

ومن الأمثلة على ذلك التنصت على مكالمة للأميرة ديانا مع صديقها جيمس جِلبي (James Gilbey)، وتسجيلها لمدة 23 دقيقة حيث نشرت في الـ (Sun)، حيث أحرجت الأمير تشالز (Neumann, 1995).

يمكن اعتراض رسائل البيجر من خلال نسخة مقلدة من بيجر أو ما يسمى (Cloned)، والذي يلتقط الرسائل من بيجر محدد، وبمبلغ يقدر (300 ـ 1000) دولار يمكن شراء هذا البيجر، وحاسب مع برمجيات خاصة به وماسح للتجسس.

لقد علقت باميلا فينكل (Pamela Finkel) على الصفحة الخاصة بها على الإنترنت فحوى مادة من رسائل البيجر المرسلة إلى الاستخبارات الخاصة بالرئيس الأمريكي بيل كلينتون، والتي تشمل تفاصيل عن زيارته إلى الفلبين في25/ 4/ 1997م، حيث أعطيت لها المادة من أحد قراصنة الحاسب، وشمل ذلك دقيقة بدقيقة لأمكنة وجوده، والتعليمات إلى الاستخبارات الخاصة، وملاحظات الحب التي كتبت له (Brekke, 1997).

إن خسارة الجوالات من التقليد حوالي (650) مليون دولار في الولايات المتحدة الأمريكية. وفي إحدى الحالات تم استخدام (1500) مكالمة لجوال واحد من قبل لصوص الجوال. ويمكن الحصول على أرقام الـ(ESN) و(MIN) من خلال رادار

(ESN) يشبه التلفون الجوال ومصمم لمراقبة وضبط القنوات، ويمكنه التقاط أرقام الزوج (Pair) . (Barry & Wilkinson, 1996) .

ومن الإجراءات الأمنية المتعلقة بالجوال أن لا يحمل الجوال عند دخول الشخص إلى أمكنة محظورة أو حساسة لأنه قد يقلب الجوال إلى ميكروفون تجسس دون علمك. ضع جوالك على وضع التشغيل فقط عندما تريد أن تجري مكالمة، أغلقه عند الانتهاء من المكالمة. لا تعط رقمك إلى أي شخص، ولا تستخدم جوالك في استقبال المكالمات. ولا تناقش معلومات حساسة من خلال المكالمة باستخدام الجوال. أعلم من تتحدث معه أنك تجري مكالمة من الجوال لكي يأخذ الحيطة في الحديث. لا تترك جوالك في أي مكان، تجنب استخدام الجوال في الأماكن العامة مثل المطار، والتجمعات الرياضية، وأماكن التسوق، أو الأمكنة المزدحمة لأن هذه الأمكنة يكثر فيها هواة الراديو الذين يمسحونها (Scan) لالتقاط الأرقام أو المحادثات.

4- **تسجيل المكالمات** (Tapping) .

يحوي التلفون جميع أنواع معدات المراقبة (ميكروفون، سلك لنقل المعلومات من المصدر إلى المرسل) ويمكن مع بعض أنواع التقنيات استخدام ميكروفون الهاتف لنقل كل المعلومات في غرفة ما وما يتم فيها من محادثة. ويمكن مراقبة المحادثات في غرفة ما من خلال الهاتف من مكان بعيد عن ذلك المكان. ومن الطرق المستخدمة في عمل مثل هذه التعديات وبعضها حتى لا يتطلب وصلاً مادياً إلى الهاتف ومنها:

1ـ استخدام أساليب صيانة نظام التلفون (أو الحاسب) لوضع الهاتف خارج القاعدة (Off-hook) .

2. استخدام برنامج حاسب خاص بنظام الهاتف يمكن جعل التلفون يجيب والسماعة مرفوعة، وهذا تفعيل عن بعد لخيار السماعة (Speaker) .

3ـ وضع مولد كهربائي خارجي أو ضابط للإشارات على خط الهاتف.

4ـ تعديل جهاز التلفون أو برنامج وحدة التحكم من خلال استغلال مخرج الصيانة عن بعد.

إن تسجيل المكالمات الصوتية يتيح المجال للمتنصتين (Eavesdropper) بمراقبة وتسجيل جميع المحادثات على ذلك الخط. ومن غير المرجح كشف تسجيل المكالمات

من قبل المستخدم خاصة ذلك النوع المعقد من التلفونات المستخدمة في التسجيل. وحتى الألياف الضوئية التي حلت محل أسلاك النحاس يمكن اعتراض المكالمات منها وتسجيلها.

5- **الفاكس** (Fax Machine).

أصبحت آلة الفاكس أداة ضرورية في العمل وفي المنزل، وهي أداة اتصالات من السهل استهدافها، وهذا يعني أن اعتراض إشارات الفاكس يتم بالطريقة التي يتم فيها اعتراض إشارات الاتصالات (المكالمات). إن أي جهاز حاسب وأي معدة لاعتراض البيانات تمكن من اعتراض والتقاط إرسال الفاكس من أي آلة، وبغض النظر عن ارتباطها مع الجهاز في الطرف الآخر. وبعض الفاكسات عرضة للاعتراض أكثر مع خاصية تخزين الفاكسات كصور ويمكن وعن بعد الوصول إلى الفاكسات المخزنة في الجهاز وهناك صندوق بريد مخفي لحفظ الفاكسات لمن يسمح له بالوصول إليها، وعادة ما تسمى رقم الهوية الشخصية (PIN) وهو رقم يمكن المستخدم المصرح له بالاستخدام استعادة الوثيقة من الفاكس بشكل إلكتروني وتحويلها إلى نسخة ورقية ويمكن بمعرفة هذا الرقم (PIN) استعادة الفاكسات المرسلة إلى طرف ثالث (Hefferman, 1992).

6- **التلفون اللاسلكي** (Cordless Phone).

يمكن التقاط إرسال التلفونات اللاسلكية في حدود الميل، ويأتي هاتف (موجي Analog) ومع ماسح راديو وفي الحي الذي تتم فيه المكالمات، ويمكن لأي شخص سماع هذه المحادثة. والميكروفونات اللاسلكية التي تستخدم في المؤتمرات والندوات كذلك لها نفس المشكلة. الهواتف الرقمية (Digital) أكثر أمناً من هواتف الموجة، كما يمكن سرقة نبضات الهاتف (Tone) من الهاتف واستخدامه في الاتصالات من لصوص الهواتف (Barry & Wilkinson, 1996).

7-**آلة الرد الصوتي** (Answering Machine).

تستخدم آلة الرد الصوتي مثلها مثل البريد الصوتي وخطورة استعمالها إنها تُمكن الدخلاء والمتطفلين وغيرهم من استخدامها عن بعد والاستماع إلى الرسائل المسجلة

عليهـا. ويمكن سمـاع الرسائل المسجلة من خارج الدولة إذا عرف الشخص الرقم الشخصي لتسجيل آلة التسجيل (Barry & Wilkinson, 1996).

8- **البريد الصوتي** (Voice Mail).

غالباً ما تستخدم المؤسسات البريد الصوتي كاسلوب في التواصل بين الإدارة والموظفين وبين الإدارة والموظفين والعملاء. ويقوم البريد الصوتي في العمل على أن يُعطى لكل موظف بريد صوتي خاص به يتلقى عليه اتصالات الآخرين والتي غالباً ما تخص العمل. وإذا ما توصل أحدهم من الداخل أو الخارج أو أحد الموظفين المفصولين أو المسرحين إلى البريد الصوتي فإنه يمكن أن يستغل المعلومات التي يحصل عليها وقد تسبب إيذاء للشركة أو المؤسسة، أو فقداناً لعملائها وكشف خصوصية العملاء مع المنظمة. وكذلك الحال فإنه يمكن خرق البريد الصوتي الشخصي، واستغلال المعلومات ضد الأفراد أو بيعها أو استخدامها.

ومن الأمثلة على خرق البريد الصوتي في المؤسسات ما قام به جون هيبل (Hebel) وهو موظف سابق في شركة (Standard Daplicating Machines Corporarion) في ماندوفر، حيث عمل هيبل كمدير مبيعات ميداني في الفترة (10/ 1990 إلى 9/ 1992) وكان يعمل من مكتب أعده في منزله في مدينة بول ون، وكان للشركة بريد صوتي ولكل موظف صندوق بريد صوتي يمكنه الدخول إليه عن بعد وتشمل الرسائل الصوتية المسجلة معلومات عن المبيعات والعملاء والطلبيات... إلخ. وبعد أن ترك هيبل الشركة ذهب إلى شركة أخرى منافسة وفي نفس المجال، وهي شركة يابانية (Duplo Manufacturing Corp.) وعين كمدير إقليمي لها في الوسط الغربي من الولايات المتحدة، وقد طور هيبل طريقة للاحتيال من خلال الدخول غير المشروع إلى نظام البريد الصوتي والدخول بمعرفته لكلمات الدخول (مفاتيح الدخول) وهي الأرقام الفرعية لتلفونات الموظفين، وتمكن من معرفة مفاتيح الدخول للبريد الصوتي لمدراء الشركة والمسؤولين فيها واستخدم المعلومات التي حصل عليها من البريد الصوتي لمصلحة الشركة المنافسة معهم ولمصلحته الشخصية. وأخيراً تمكنت (FBI) من اعتقاله وسجنه سنتين تحت المراقبة (Freeh, 1996).

9 -**اعتراض الاستخبارات الأجنبية**

تهتم أجهزة الاستخبارات بجمع المعلومات عن الأفراد والمؤسسات والحكومات الأجنبية والتي تمثل اهتماماً، أو تهديداً للأمن الوطني للدولة. وفي الولايات المتحدة

لا يسمح لهذه الأجهزة بالتجسس على المواطن الأمريكي (قبل إحداث 9/11) ولكن مسموح لها التقاط مكالمات الأشخاص الأجانب خارج الولايات المتحدة. فمثلاً تقوم وكالة الأمن الوطني (National Security Agency [NSA]) بجمع المحادثات التي تهم الأمن الوطني الأمريكي والمتعلقة بالإرهاب، ومبيعات الأسلحة، والمخدرات، والصفقات التجارية . . . إلخ. ففي عملية تجسس على المكالمات قامت بها السفارة الأمريكية في كاركاس، فنزويلا تم ضبط (12240) كغم من الكوكايين المشحون إلى فلوريدا، وكانت ثاني أكبر عملية مصادرة كوكايين في الولايات المتحدة. ولقد تم تطوير عدة أدوات لهذه الأغراض، فيما سمي بمشروع يوجارت (Yogurt)، طورت أداة تشمل باحثاً، ومستقبل راديو، وحاسباً، ومسجلاً في وحدة واحدة.

وتستقي (NSA) جزءاً من معلوماتها الدولية من خلال المشاركة في إيكولون (Echelon)، وهو نظام مراقبة عالمي تشترك فيه خمس دول هي الولايات المتحدة، وبريطانيا، وكندا، وأستراليا، ونيوزيلاندا. وهو شبكة من وسائل الاستماع والتنصت بما في ذلك اعتراض محطات الستالايت، ومحطات الميكروويف الأرضية، وستالايت التجسس، ومحطات الاستماع للراديو، والمواقع السرية، وهذا الكم الهائل من اللاقطات الهوائية ومعدات الاعتراض قادرة على التقاط الصوت، الفاكس، والبيانات المرسلة، والمتناقلة عبر العالم.

وأكبر المحطات منوث هل (Menwith Hill) (المحطة الأرضية F83) وتدار من قبل (NSA) في نورث يورك مورز (North York Moors) في شمال بريطانيا، وتشمل (22) ستالايت على (5) أفدنة من المباني وتعمل كمحطة تجسس أرضية أمريكية، حيث تعترض خطوط الميكروويف والاتصالات بالموجات القصيرة، والإتصالات العسكرية. أما المحطات الأخرى فموجودة في سوجار جروف (Sugar Grove) في غرب فرجينيا، ياكيما (Yakima) في ولاية واشنطن، ومورونستو (Morwenstow) في بريطانيا، وجيرالدون (Geraldton) في غرب أستراليا، أيهوبيا (Waihopai) في نيوزيلاندا. وهناك أنظمة ضبط وتحكم منظمة تقوم باعتراض الرسائل الإلكترونية والإتصالات وتصنيفها ضمن فئات، وهناك قواميس مبرمجة أن لا تعترض الاتصالات الصادرة من الدول الخمس. أما الفئات المعترضة من الرسائل فتركز على السياسة والشؤون العسكرية (Compbell, 1996).

ولقد أقامت روسيا واحدة من أكبر محطات التجسس على الاتصالات بالقرن من هافانا في كوبا في السبعينيات بقصد اعتراض الاتصالات العسكرية والدبلوماسية

والتجارية في شرق الولايات المتحدة، وجزء من الوسط الغربي. ويمكن لهذه المحطة التقاط اشارات الخلوي، والميكروويف، والراديو على مسافة (1000)ميل. أما الاتصالات في غرب الولايات المتحدة فتعترض من محطة مشابهة في كام رانه بي (Cam Ranh Bay) في فيتنام. ويقول ستنيليف لونيف (Stanislav Lunev) أحد كبار مسؤولي الكرملن أن خطط الأمريكان العسكرية واتصالات الجنود مع أسرهم في حرب الخليج قد تم التقاطها من قبل محطة لوردز (Lourdes). (Associated Press, 1998).

10- **حل رموز الرسائل** (Deciphering Messages)

لا يتوقف دور أجهزة الاستخبارات على اعتراض الرسائل بل وحل رموز تشفيرها (Deciphering). ومن الأمثلة المعروفة على حل (فك) رموز الرسائل المشفرة ما حدث قبل دخول الولايات المتحدة للحرب العالمية الأولى، ففي عام 1917 أرسل وزير الخارجية الألماني آرثر زمرمان (Arthur Zimmermann) رسالة مشفرة (تلغرام) إلى السفارة الألمانية في مدينة ميكسيكو (Mexico)، حيث تم اعتراض الرسالة وفكها (Cryptanalzed) من قبل مفككي الشيفرة الإنجليز في (الغرفة 40) كانت موجه إلى الحكومة المكسيكية وتقول :

«ننوي شن حرب غواصات في الأول من فبراير وننوي إبقاء الولايات المتحدة محايدة، وإذا ما نجح ذلك فإننا نجعل المكسيك حليفاً على الأسس التالية : القيام بالحروب معاً، القيام بالسلام معاً، الدعم المالي السخي، وفهمنا حاجة المكسيك لإعادة أراضيها في تكساس، ونيومكسيكو، وأريزونا . . . .»

وقام الإنجليز بإعطاء نسخة من هذه الرسالة إلى ولسون (Wilson)، وحيث نشرت في الصحافة حيث هزت الرأي العام الأمريكي، ووصفها ولسون إنها «جريمة ضد الإنسانية» أن تقود بلداً إلى الحرب في إشارة إلى تلغراف زمرمان، طالباً من الكونجرس إعلان الحرب على ألمانيا، وقد فعل مما سبب دخول الولايات المتحدة إلى الحرب وأدى إلى هزيمة ألمانيا (Kahn, 1967).

وخلال الحرب العالمية الثانية قامت الولايات المتحدة بفك شيفرة اليابانيين مما أدى إلى انتصار البحرية الأمريكية في بحر الكورال (Coral Sea)، وجزر السولومون

(Solomon Islands)، وكان يمكن تلافي الهجوم على بيل هاربر (Pearl Harbor) من اليابانيين لو عولجت الرسائل بسرعة، ولكن عند كشف محتواها كان قد فات الأوان. وبعد أقل من سنتين التقط (Eavesdroppers) جدول رحلات الأدميرال اسكوروكو ياماموتو (Isoroku Yamamoto) رئيس هيئة أركان البحرية اليابانية، وقامت المقاتلات الأمريكية بتدمير طائرته في الجو. ومن المشاريع الأمريكية الأخرى مشروع فينونا (Venona)، والتي اعترضت وفكت رموز البرقيات الدبلوماسية الروسية في الفترة 1942ـ1946. حيث كشف المشروع الجواسيس الروس من الأمريكان وأدى اعتقال وإدانة الكثير، ومنهم جوليوس (Julius)، وايثيل روزنبرغ (Ethel Roseuberg)، والذين زودوا الاتحاد السوفياتي بما تقوم عليه القنبلة الذرية وتفاصيل المقاتلات، والرادار والصواريخ (Dam & Lin, 1996).

ومن الكوارث التي أصابت القادة العسكريين خلال الأيام الأخيرة للحرب في الباسيفكي أنه في شهر 7/ 1945م حيث كانت انديانابولس (Indianapolis) في طريقها إلى الفلبين بعد إرسالها الوقود الذري ومكونات القنبلة الذرية والتي ألقيت فيما بعد على هيروشيما وناكازاكي الشهر التالي، وبينما كانت السفينة تبحر في مياه العدو تمكن قارب ياباني سريع من إصابتها وإغراقها في دقائق وتدمير نظام الراديو فيها، وقفز (800) من أصل (1196) شخص إلى السطح نجا منهم (316) فقط، أما البقية فغرقوا، أو قتلوا من أسماك القرش. وفاتت خمسة أيام قبل أن تجدهم السفن الأمريكية وبالصدفة. أما قبطان السفينة الكابتن تشالز مكافي (Charles McVay) فصدر بحقه حكم في المحكمة العسكرية بسبب فقدانه للسفينة، وفي عام (1968) انتحر بمسدسه الرسمي. وبعد (50) سنة بين طالب عمره (12) سنة يدعى هنتر سكوت (Hunter Scott) أن رئيس مكافي كان يعلم مسبقاً بوجود غواصة للعدو قريبة من انديانا بولوس، وتم إغراق سفينة أمريكية أيام قبل ذلك الحادث، ولكنه لم يحذر الآخرين، وتبين أن طلب مكافي للحماية لم يوافق عليه، ولم ترسل القاعدة في الفلبين فريق إنقاذ عندما لم تصل انديانابولوس في الوقت المحدد، لقد وجد هذه المعلومات من خلال مشروع في التاريخ يقوم به (Gurdon, 1998).

11- **الإرسال بالستالايت** (Satllite Transmissions).

عندما يستخدم التلفون أو الفاكس، فإن مجرى هذه الإرسالية يسير إما من خلال الخطوط الأرضية، أو الميكروويف الأرضي الذي يعتمد على الأبراج أو بواسطة

الستالايت. إن غالبية الاتصالات الدولية تسير (على الأقل في مرحلتها الأخيرة) من خلال الأمواج الهوائية ـ من خلال الستالايت أو بين أبراج الميكروويف ـ وأي شيء في الفضاء يمكن اعتراضه. إن التقنية اللازمة لمراقبة الاتصالات عبر الميكروويف والستالايت كانت باهظة الثمن ومعقدة. أما هذه الأيام فإن أي مجموعة أفراد يمكنهم الحصول عليها، وقد أصبحت هذه المواد والمعدات متاحة للعامة (Off-the Shelf).

ومع تعقد وسائل الاتصال وتطورها فإنه بالإمكان إجراء العديد من الاتصالات في آن واحد ومن خلال معدة واحدة. ولازال من السهولة بمكان ترتيب وتعقب ملايين المكالمات والفاكسات والبيانات المرسلة لتحديد الشخص المستهدف ومن خلال الكلمات المفتاحية لتحديد الشخص المستهدف.

وتسير المكالمة الهاتفية أو الفاكس المرسل من المرسل بواسطة الخطوط الأرضية، أو الميكروويف الأرضي إلى محطة التغير، فمن الحاسب الخاص بشركة الاتصالات الذي يربط الاتصال (المكالمة أو الفاكس) مع الستالايت وترسل إلى المحطة الأرضية وترسل إلى الستالايت مرة أخرى إلى المحطة الأرضية ومن ثم تسير من خلال الخطوط الأرضية أو الميكرويف إلى محطة التغير ويتم فصلها عن بقية الإشارات ومن خلال الخطوط إلى تلفون الشخص المستقبل وتحويلها إلى صوت أو فاكس. كل هذا يحصل في أجزاء من الثانية.

إن التحميل من الستالايت يسهل اعتراضه لأن إشارة الميكرويف تذهب في جميع الاتجاهات، وكلما كانت الستالايت عالية كلما زادت المساحة على الأرض للستالايت (تسمى بصمة القدم) التي يمكن التقاط موجة الراديو تلك وبالتالي اعتراضها.

إن أي شخص ضمن بصمة القدم وبلاقط ستالايت (دش) وبعض المعدات المتوافرة يمكن التقاط تلك الإشارات بالطريقة ذاتها التي يلتقطها لاقط الستالايت ويحولها إلى إشارات التلفزيون. ويمكن التقاط إشارات الستالايت من السفارات أو المباني المملوكة للأجانب أو من السفينة في البحر.

تستخدم محطات الميكرويف الأرضية لنقل الاتصالات الدولية للدولة ويستخدم حالياً الاتصالات عبر الستالايت. أو خطوط الألياف الضوئية وتستخدم الميكرويف

الأرضية للاتصالات عبر مسافات قصيرة بين مكاتب التلفونات المحلية، وتوزيع محطات إرسالها على مسافات (25ـ30) ميلاً بين كل برج والآخر ذلك أن الإشارات المرسلة تسير في خط مستقيم ولا تتبع منحنى الأرض. وهذه الإشارات سهلة الاعتراض من أي شخص يقع ضمن مداها وبالأدوات المتوافرة. وأحد عيوب الإرسال بالميكروويف سواء كان أرضياً أو بالستالايت هو أن الإشارات (Beams) لها جانب دوران (Side lobes)، أو دوران (Spill) على المساحة كلها بين أي نقطتي إرسال. وباستخدام بعض أنواع اللاقطات فمن الممكن اعتراض الإشارة من الجانب إذا كان هناك خط نظر مباشر بين الجزء والإشارة (خالٍ من العوائق كالمباني) ولذلك تختار السفارات مواقعها في أمكنة تمكنها من الاعتراض.

12-**الفيديو** Vidio

مع انتشار كاميرات الفيديو علي نطاق واسع، فقد مكنت هذه الادوات من الحماية كما هو الحال في المجال التجارية الكبيرة أو المنازل، ومع تقدم هذه التقنية فقد أصبحت بحجم صغير جداً ويمكنها البث اللاسلكي وبسعر رخيص جداً في حدود ال (50) دولار، ويمكن ربط هذه الكاميرات مع الانترنت بحيث تمكن الشخص من المراقبة عن يُعد للموقع المعني ويمكنها البث والتقاط الصور من أمكنة بعيدة، وإذا مازرعت هذه التقنية في مكان ما، فإن الشخص يتمكن من تسجيل وتصوير ما يحدث في ذلك المكان ومن أي مكان.

13-**التنصت على المحادثات الهاتفية** (Eavesdropping on Conversation)

إن غالبية إشارات (Signals) الاتصالات مكشوفة للاعتراض، وبعضها وبجهد بسيط يمكن اعتراضها، والبعض الآخر يتطلب اعتراضها أدوات معقدة. ومن أدوات الاعتراض الكثيرة الميكروفونات الصغيرة (Bugs)، والمسجلات، ومعدات التسجيل، والماسحات الخلوية، والراديو، والميكروويف، والفضائيات، وفضائيات التجسس، والشمام (Sniffer)، والمصافي (Filters) لعزل المعلومات ذات الاهتمام. ويمكن للميكروفونات المسماة (Parabalic) اكتشاف المحادثات على مسافة كيلومتر، والميكروفونات الليزر يمكنها التقاط محادثات خلف الجدران.

ومن الأمثلة ما قام به بوليسن (Poulsen) في التنصت على مكالمات الآخرين باستخدام آلة تسمى (SAS) حيث تمكن التقاط للمكالمات عن بعد، وتمكن كذلك من

معرفة التلفونات المراقبة من غير المراقبة، وفي مدة (90) دقيقة تمكن من تحديد جميع التلفونات المراقبة في الولايات المتحدة من قبل الـ(FBI). (Littman, 1997).

على الرغم من أن التنصت سلوك غير قانوني إلا أنه شائع الاستخدام من قبل الأجهزة الأمنية عامة، بعضها بغطاء قانوني من مثل أمر محكمة شكلي، أو فعلي، وبعضها دون أي غطاء قانوني كما هو الحال في غالبية الدول النامية. والأساس هنا هو أن التنصت غير القانوني فيه خرق للخصوصية الفردية (Protection of Privacy).

تستخدم المراقبة الإلكترونية وخاصة اعتراض المكالمات الهاتفية في التحقيقات الجنائية بما في ذلك الجرائم المنظمة، وتهريب المخدرات، والفساد العام. ويعد التنصت باستخدام تسجيل المكالمات الهاتفية مفيداً لأنه يظهر الكلمات والأقوال والخطط والنوايا للفاعلين. ففي أحد العمليات لملاحقة تهريب المخدرات في مدينة نيويورك، حيث قامت إلـ (FBI)بـ (55) حالة مراقبة نجم عنها اعتقال (222) حالة، وإدانة (167) حالة (Freeh, 1994).

في عام 1997م أقرت المحكمة (1186) طلباً للتنصت على المجرمين منهم (73%) مخدرات خطرة تشمل جرائم متعددة، (8%) قمار (Gambling)، والابتزاز المالي (Racketeeing). ومن حالات التنصت كان هناك (69%) اعتراض للمكالمات الهاتفية، أما الوسائل التقنية الأخرى مثل البيجر، والخلوي، والبريد الإلكتروني فقد بلغت (19%) من الحالات، والميكروفونات (3%)، وأما بقية الوسائل المتعددة فشملت (9%) من الحالات. كانت الكلفة الإجمالية لهذه العمليات (61176) دولار غالبيتها كانت أجرة عمل (Aousc, 1996).

الاحتيال في الاتصالات الهاتفية (Telecommunications Fraud)

هناك عدة أنواع للاتصالات الهاتفية فمنها سوء استعمال الهاتف (Teleabuse)، والاحتيال في الاتصالات المجانية (Toll Fraud)، والدولية، والاحتيال في اتصالات الجوال، ومن أكثر الأنواع خطورة استعمال أرقام الآخرين في الاتصال، وتسجيل المكالمات باسمهم مما يؤدي إلى احتساب كلفة هذه المكالمات على أصحاب الهاتف، وتقدر خسارة هذا النوع من الاحتيال في الولايات المتحدة في عام (1997) (15) مليون دولار (CSI/FBI, 1998).

وهناك طرق أخرى متعددة لسرقة الخدمات الاتصالية مثل سرقة الصناديق الزرقاء (Blue Boxes) والتي تعمل على طنين (2600)، وبالتالي فإن وضع أي جهاز إرسال في الصندوق وربطه بالهاتف، أو بخط الهاتف يُمكن من سرقة خدمة الاتصالات. كما أن هناك طرقاً لسرقة الخدمات الاتصالية على نفقة الشركة صاحبة الخط من خلال الوصول إلى الصندوق الخاص بالشركة والمعروف Private Branch Exchange) ([PBX]، ويعد الاحتيال في مجال الاتصالات الهاتفية جذاباً لعدة أسباب:

1ـ مستوى الخطورة المتدني بالنسبة للمحتال، فاحتمالية أن يدان، أو يلقى القبض على الشخص احتمال ضعيف. ويمكن تنفيذ العمل عن بعد ومن الصعب كشفه وملاحقته.

2ـ لا توجد حاجة إلى معدات خاصة لتنفيذ العمل.

3ـ هناك مردود مالي من بيع المكالمات الهاتفية للآخرين (طرف ثالث) (Hoath, 1998).

وهناك عدة أنواع من الاحتيال في الاتصالات، ومنها على سبيل المثال :

1 ـ **الاحتيال في البريد الصوتي** (Voice Mail Fraud): يشمل الاحتيال في البريد الصوتي سرقة رموز الدخول (Access Codes)، للشركات، وسرقة كلمات الدخول، وأرقام الهواتف، وأرقام بطاقات الائتمان، والإتصالات الدولية . . . إلخ. ، وبالإضافة إلى إستخدام هواتف المنظمة الضحية في الاتصالات يمكن سرقة الأسرار التجارية ومن الأمثلة على مثل هذا الاحتيال ما حصل في عام 1989 لشركة العقارات في إلينوي حيث قامت لسلي لن (Leslie Lynne) في الاحتيال على البريد الصوتي للشركة وتوزيعه على (52) من قراصنة الحاسب، حيث سرقت (481) رمز دخول (بطاقات ائتمان، وأرقام هواتف . . . إلخ). وقدرت الخسارة (595941) دولاراً (Cook, 1991).

2 ـ **الاحتيال في بطاقات الاتصال** (Calling Card Frqud) : يشمل الاحتيال في بطاقات الاتصال الهاتفية الاستخدام غير المصرح به لبطاقات اتصالات الهاتف، وعادة ما يتم بيع هذه الأرقام. وتتركز سرقة الأرقام هذه من خلال الهواتف المتوافرة في المطارات حيث غالباً ما يستخدم المسافرون هذه البطاقات ويمكن إلتقاط أرقامهم ومن ثم الاتصال على نفقتهم.

3 ـ **الاحتيال بتلفونات الجوال والاحتيال بالهواتف المقلدة:** يتضمن الاحتيال في هواتف الجوال الاستخدام غير المصرح به، والاحتيال في استخدام تلفونات الجوال، وهذه تشكل مصدراً هاماً في الخسارة المالية. وتأتي غالبية الخسارة من ما يسمى بالتلفونات «المزورة» وهي تلفونات مقلدة (Cloning) وهي طبق الأصل عن التلفونات، وبالرقم ذاته المعطى للزبون. وعندما تنفذ المكالمة من خلال التلفون المزور ترسل الفاتورة إلى صاحب الهاتف الأصلي. وتسهل عملية نسخ الهواتف الموجية (Analog) بمساعدة ماسحات (SEN/MIN) والتي تلتقط الرقم الإلكتروني المتسلل للهاتف (ESN)، والرقم المحدد للجوال (MIN)، والذي يرسل من خلال عملية التجهيز الأولية للهاتف. وهناك أدوات أكثر تعقيداً من مثل صندوق اعتراض البيانات الرقمي (DDIB) الذي يمكن من التقاط الرموز السرية للهاتف (PIN)، وعندما يتم التقاط هذه المعلومات يتم تخزينها في الهاتف «النسخة»، ويتم تسجيل المكالمات على صاحب الهاتف الأصلي.

ويمكن الوقوف قرب أمكنة الإرسال المزدحمة حيث تتمكن ماسحات (ESN/MIN) من التقاط العديد من أزواج الأرقام ويمكنها من حصد الكثير من هذه الأرقام واستخدامها غير الشرعي. وتعد مشكلة استنساخ (تقليد) الهواتف (Cloning) خاصة مع الهواتف الموجية والتي لا تستخدم التشفير لحماية اتصالاتها من الاعتراض. أما الهواتف الرقمية فمحصنة، وتباع الهواتف المستنسخة في السوق السوداء لمروجي المخدرات، وتجارها، حيث يسرقون أرقام السرية، ففي إحدى الحالات قام تجار المخدرات في كولومبيا باستخدام هواتف الشرطة في الاتصال، حيث تدفع الشرطة فواتير الاتصال حيث استخدمت هواتف إدارة مكافحة المخدرات (DEA)، (Ramo, 1996).

مراقبة شبكات الحاسب

تستخدم مراقبة شبكات الحاسب لأغراض حرب معلومات دفاعية وهجومية للمعلومات، فعلى الجانب العدواني فإن الدخلاء على الشبكات يسترقون السمع للاتصالات على الشبكات، وفي الجانب الدفاعي فإن إدارة الشبكات تتعقب نشاطات

(1) الشمامون (Sniffers) استعارة أخذت من بحوث الطلاب البولوسية عن الادلة أو عن المخدرات، وهي هنا تعني برامج مخصصة للبحث عن بيانات مفيدة من الشبكات لاستخدامها لتحقيق أغراض وفوائد شخصية.

الدخـلاء و الداخليين الذين يسؤون استـخدام شبكاتهم، ومن أهم وسـائل مراقـبة شبكات الحاسب الآتي :

1 ـ **شمامو الحزم المعلوماتية** (Packet Sniffers) : غالبية شبكات الحاسب عرضة للاعتراض من الشمـامين (1)، ويجمع الشمـامون المعلومات من خلال تنقلهم على الشبكة، واصطياد رزم البيـانات، حيث ان الرسائل الإلكتـرونيـة تقسم إلى رزم (Packets) قبل إرسالها، وفي نهاية الاستقبال يعاد تجميعها بشكل رسائل متكاملة. وتستخدم "رزم الشم" من قراصنة الحاسب لالتقاط المعلومات،وتستخدم من قبل إدارة الشبكات لابعاد قراصنة الحاسب عن الشبكة، ومن قبل المحققين لتعقب أنشطة القراصنة.

ولقد تمكنت الأجهزة الأمنية الفدرالية الأمريكية من الحصول على أول أمر محكمة لتسجيل (تنصت بالتسجيل الصوتي) على شبكة حاسب، وتعقب طالب أرجنتيني تمكن من القرصنة على نظام الحاسب في جامعة هارفرد، ولقد استخدم نظام الحاسب في الجامعة كمصدر منه تمكن من الدخول إلى الشبكات الأخرى منها نظم الدفاع في البحرية ومركز الضبط والمراقبة في سان دياغو كاليفورنيا، ومختبرات البحوث البحرية في واشنطن . . . إلخ. وكـذلك تمكن من الولوج إلى حـاسـبـات في كـوريا، والمكسيك، وتايوان، وتشيلي، والبرازيل. وبواسطة برمجيات الشم تم التمكن من تحديد جيوليو سيزار ارديتا (Julio Cesar Ardiat) وعمره (21) سنة، وهو طالب جامعي، وابن لضابط متقاعد. وحكم عليه بالسجن (3) سنوات، وغرامة (5.000) دولار (Ferdinard, 1998).

2 ـ **مراقبة إدخال المفاتيح** (Keystroke): تعني مراقبة إدخال المفاتيح واعتراض كل نقرة على لوحة المفاتيح من الفرد، وعادة ما تستخدم من إدارة الشبكات والمحققين لتعقب الدخلاء على الشبكة.

3- **تحليل المرور الإلكتروني (الذروة)** (Traffic Analysis): تحمل الاتصالات الإلكترونية عبر الشبكات والتي تشمل الهاتف، وشبكات الحاسب نوعين من المعلومات:

1ـ محتوى الرسالة.

2ـ معلومات تجهيز الاتصال (Call-Setup)، وهذه تحدد الشركاء في نهاية الاتصال، وتشمل رقم الهاتف المتصل، وعقدة الإنترنت، أو العنوان الإلكتروني، والشيفرة (الكود) الذي يحدد الحاسب، ومعدات الاتصال، والمؤسسات. ويمكن أن تحدد مثل هذه المعلومات نمطية الانسياب الإلكتروني للمعلومات، ويمكن ما يسمى تحليل المرور الإلكتروني (مسترقو السمع Eaveseropper) من تحديد العلاقات والتغير في نشاطات الاتصال. ويمكن استخدام برامج متوافرة لدى المؤسسات الأمنية مثل المفترس (Carnivore) لتحليل محتوى الرسائل الصادرة، والواردة، والاتصالات من على خادم معين (US Today, 2001).

أ- اعتراض الاتصالات القادمة وتعقب الصادرة :

يمكن اعتراض معلومات الاتصالات واستخدامها في التحقيقات الجنائية خاصة عندما لا يكون هناك حاجة إلى التنصت بالتسجيل الصوتي، ويعطي (Pen register) الوكالات الأمنية الوصول إلى أرقام الهواتف المتصل بها من هاتف الشخص المعني. وتوفر خاصية الشراك والتعقب (Trap and Trace) معرفة الأرقام المتصلة برقم هاتف الشخص المعني مثل رقم المتصل (Caller ID). ويتطلب كلا هذين النوعين أمراً من المحكمة للقيام بالتجسس. ولا يتوقف الاعتراض والتعقب على المكالمات الهاتفية، بل يشمل المرور على الشبكات الحاسوبية، حيث يمكن تعقب الرسائل الإلكترونية حيث يمكن تحديد الشخص ومكانه من خلال تحديد رقم الحاسب.

ب- تتبع الموقع (Location Tracking):

يمكن استخدام أنظمة هواتف خلوية (جوال) لتعقب موقع المتصل وأرقام هواتف الاتصالات حتى عندما لا يكون الهاتف في وضع تشغيل، ويمكن تحديد موقعه إن كان في وضع تشغيل ويمكن تحديد الموقع الجغرافي للمتصل.

4-**كلمات الدخول** (Passwords): كلمة الدخول أو كلمة السر أو كلمة المرور هي مفتاح المستخدم للدخول إلى الحاسب على الشبكة أو الإنترنت. وهي مزيج من الأحرف والأرقام التي يضعها المستخدم ليتمكن من الدخول إلى الحاسب، وهي تمثل بطاقة الهوية التي يتعرف بموجبها الحاسب على الشخص ويسمح له بالدخول

كمستخدم شرعي. وإذا ما توصل شخص ما لهذه الكلمات فإنه يمكن أن يستخدم الحاسب، وبالتالي ينتحل شخصية ذلك المستخدم، ويفعل ما يشاء بمحتويات الحاسب أو الحساب الذي اخترقه من خلال معرفته لكلمة الدخول. كما يمكن أن يرسل الشخص المتعد رسائل كراهية للناس باسم صاحب وذلك الحاسب أو البريد الالكتروني.

ومن الأخطاء الشائعة في هذا المجال أن يكتب الأشخاص كلمات دخول سهلة التخمين من الآخرين مثل اسمه، أو اسم أحد أولاده، أو اسم زوجته . . . إلخ. وهذه المعلومات متاحة للآخرين من خلال المصادر المتاحة أو المفتوحة وبالتالي يسهل على الدخلاء محاولة تحديد كلمة الدخول إن كانت كتبت من هذه الكلمات.

أما مواصفات كلمات الدخول القوية فتشمل أن تكون على الأقل (8) أحرف وأرقام، وأن تحتوي على الأحرف والأرقام والأحرف العليا والأحرف الدنيا، والرموز الخاصة (مثل ٪ @ # $). وأن لا تكون أسماً أو جزءاً من اسم أو عنوان. وأن تكون قادراً على كتبابتها بسرعة وان يتم تغيرها على الأقل كل (90) يوماً. ويمكن معرفة جـــودة كلمـــة من خـــلال مـــوقع (www.symantec.com/avcenter / securitv /passwords /passwordcheck.html) ، وهو موقع فيه برنامج يستطيع تخمين كلمة الدخول، وهذا مؤشر على أن الآخرين يستطيعون خرق أو تخمين كلمتك أم لا.

فكلمة الدخول المكونة من (6) أحرف عليا، أو صغرى لها (308) مليون احتمال لتحديدها، أي أن إمكانية معرفتها تتطلب (308) مليون محاولة، ولكن هذه العملية لا تأخذ سوى دقائق بسيطة لبرنامج الدخلاء لكي يحددها. وعند مزج أحرف عليا وأحرف دنيا، فإن الاحتمالات ترتفع إلى (19) مليار احتمال، وإذا رفع عدد الأحرف إلى (8) أحرف يصبح عدد الاحتمالات (53) ترليون، وإذا حل رقم محل أحد الأحرف يرتفع عدد الاحتمالات إلى (218) ترليون، وبالتالي تزداد صعوبة تحديد كلمة المرور أو الدخول (NSIA, 1998).

5- **المودم** (Modem) : إن وجود الحاسب وحده لا يحمل الكثير من المخاطر أو المشكلات، ولكن عند ربطه بشبكة أو بالمودم يزيد من مخاطر اختراقه، وإساءة استعماله، وتخريب بياناته، واستغلالها. المودم أداة (معدة) اتصال تمكن الحاسب من

الوصول إلى حاسب آخر من خلال خط التلفون ومع التطورات التقنية الآن فإنه يمكن تحويل الحاسب إلى أداة اتصال تحل محل الهاتف، فيمكن استخدام الحاسب كفاكس وتلفون وتلغراف ببث مباشر بين جهاز وآخر. والمشكلة أن المودم أكثر عرضة للاختراق وبالتالي فإن الحاسب ومحتوياته عرضه للاختراق كذلك.

ويستخدم الدخلاء أداة معروفة عبارة عن برنامج حاسب يقوم بطلب أرقام الهواتف تلقائياً ضمن مدى معين من الأرقام، خاصة وأن بعض المؤسسات تقع أرقامها ضمن مدى معين، وعن طلب جميع الأرقام ضمن مدى معين فإن هذا البرنامج يحدد الأرقام المتصلة بالحاسب (أرقام هواتف المودم) ويحدد بعض الخصائص الخاصة بالمودم. ويمكن الحصول على هذا البرنامج من الإنترنت مجاناً.

ففي إحدى الاختبارات قام الحاسب بطلب (1500) رقم في (16) ساعة وحدد (55) مودم، وكإجراء وقائي تقوم بعض المنظمات بوضع معدات تكشف الاتصالات المتكررة والمتصلة (إعادة الاتصالا) وتقفلها، وبالمقابل بعض برامج ورداييلر مصمم لتجنب هذه الخاصية (Behar, 1997).

نجحت مجموعة الدخلاء في خرق نظم الحاسب الحكومية والدفاعات الإلكترونية التي تحمي المعلومات الحساسة. وهناك إشارات إلى أن بعض هذه الجماعات مدعومة من الاستخبارات الأجنبية. فلقد وظفت ال كي. جي. بي (KGB) في الفترة (1986 ـ 1989) مجموعة من الألمان بالدخول غير المشروع إلى النظم الحكومية الأمريكية. ولقد تم خرقهم لنظم وزارة الدفاع (Pentagon) وشبكات ناسا (NASA) ومختبرات ألاموس الوطنية (Alamos [ANL])، ومختبرات لورنس بيركلي. ولقد تم كشفهم من قبل ستول (Stoll) في بيركلي عندما كان يتفحص بعض الفروقات في فواتير الحسابات وبعدها ألف كتاباً حول تلك الحالة. ولقد تم اعتقال الثلاثة دخلاء وتمت إدانتهم بالتجسس (The Washington Post, 1996).

6- **الحرمان من الخدمة** (Denial of Service [DOS]).

لا تتوقف الثغرات الأمنية في الاتصالات على الدخول غير الشرعي، أو الولوج إلى النظام، ولكن إلى الحرمان من الخدمة بالنسبة للعملاء أو الزبائن، ويحدث هذا عندما تزدحم خطوط الهاتف بالنفايات من البيانات التي لا تستخدم للعمل، وهذا

مشابه إلى الفيضانات في البريد الإلكتروني (Moynihan, 1987). وهناك أربع فئات من التعديات التي تؤدي إلى الحرمان من الخدمة وهي توقيف الخادم، وتوقيف دوائر وحدة المعالجة الرئيسة (CPU)، أوالمصادر، وتعطيل حركة الوب، والقنابل البريدية، بالإضافة إلى ذلك فهناك أنواع أخرى منها فيضانات التزامن (Syn flood)، وأزيز الموت (Ping of Death)، وتشغيل النظام المضيف والحرمان من الخدمة بالصدفة.

المراقبة البيئية (Environment Surveillance):

هناك العديد من من المجسات المتسخدمة لجمع المعلومات من البيئة الفيزيقية، بما في ذلك الكاميرات، ونظم الصور والخيالات، ومن أهمها:

1ـ **الكاميرات والفيديو** (Cameras & Video) : غالباً ما تستخدم الكاميرات والفيديو في المؤسسات التجارية كأمكنة التسويق والبنوك، وأحياناً بعض المؤسسات الحكومية، والمنازل، والمطارات، وكراجات السيارات، وذلك لمنع السرقات، أو السطو، أو التسلل، أو التعديات . . . إلخ. من أنواع الجرائم المتوقع حدوثها في مثل هذه المواقع. ويمكن النظر إلى هذه الأدوات على إنها أدوات دفاعية في حرب المعلومات ضد الجريمة، والهدف هنا جمع معلومات عن سلوك المنحرفين.

ولقد أظهرت أنظمة المراقبة بالفيديو فعالية خاصة في المناطق المتوقع أن ترتفع فيها الجريمة من مثل وسط المدينة، وأمكنة التسوق الكبرى . . . إلخ. فقد أظهرت شرطة بلتمور انخفاض (33%) من حالات الجريمة بعد تطبيق نظام المراقبة الفيزيقية. كما تم خفض دور الدعارة من (44%) إلى (6%) بعد ما تم تعميم صور البغايا المأخوذة بكاميرا الفيديو (Fehr, 1997).

وقد استخدمت الشرطة في بعض الولايات المتحدة نظام التصوير بالفيديو لمراقبة قاطعي الإشارات الضوئية الحمراء كما هو في فاري فاكس في ولاية فرجينيا، حيث يتم إرسال المخالفة مع الصورة (50 دولار) وفي مدة حوالي (6) أشهر وتم ضبط (4589) حالة في ثلاثة قطاعات منها (863) ثم دفع مخالفاتها (Moreno, 1997).

2ـ **الستالايت** (Satellites): يمكن للستالايت أن تزود بصور ذات كلفة منخفضة من الطائرات، ولم تعد مثل هذه الصور حكراً على الحكومات، فمنذ التسعينيات بدأ

الروس ببيع مثل هذه الصور من خلال وكالة الفضاء الروسية، حيث أنه وباستخدام المعدات اللازمة يمكن التمييز بين الشاحنة والسيارة، ويمكن للمهتمين مشاهدة بعض هذه الصور على الإنترنت قبل شرائها، ويعالج موقع تيراسيرفر (Terra Server) تيرا بايت (Terabyte) من البايتات (1000 جيجا بايت).

ومن المواضيع ذات الحساسية هو ضبط التصوير، وتحديد حجم وتوزيع الصور (Images) لمناطق جغرافية معينة، فقد أعلن عام (1998)م، أن الستالايت الأمريكية لا تسمح بأخذ صورة كبيرة من التركيز لإسرائيل، والخوف من وقوع هذه الصور في أيدي دول معادية، كما أن الولايات المتحدة لا تسمح ببيع مثل هذه الصور عن الولايات المتحدة إلى كوريا الشمالية، وكوبا، والعراق، وليبيا (Simons, 1998).

3 ـ **لاقطات فان إيك** (Van Eck Receptors): يمكن اعتراض ما يصدر عن لوحات مفاتيح الحاسب، الطابعات، الفاكسات، أو أي معدة إلكترونية تعطي إشارات كهرومغناطيسية، حيث تعطي الشاشة إشارات قوية وبالمعدات المناسبة يمكن للمتطفل أن يرى صورة (نسخة عن) تلك الإشارات للحاسب موضع الهجوم.

وفي عام (1985)م، توصل العالم الدنماركي وم فان ايك (Wim Van Eck) أنه يمكن تحديد المسافة القصوى باستخدام مستقبل تلفزيون بحوالي 1كم. وقد سميت الإشارات الصادرة عن هذه المعدات بـ(اشعاعات فان إيك). وقد استخدمت هذه الظاهرة في رصد أرقام بطاقات الائتمان بالقرب من البنك أو من أمكنة الصرف.

4 ـ **المجسات الأخرى** (Miscellaneous Sensors): من الأدوات الأخرى كاشف الرادار (Radar Detector) والمستخدم في القطاعات العسكرية لتحديد أمكنة الأعداء، وكذلك المستخدم من قبل الأجهزة الأمنية، وخاصة في تحديد سرعة المركبات. وبعض أنواع الرادارات تعمل على تعطيل، وتشويش على الرادارات الأخرى.

وتمكن مجسات الأشعة تحت الحمراء (Infrared) من التصوير للأجسام الساخنة ضد الخلفية الباردة والعكس بالعكس، حيث يمكن أن تعمل في الليل. أما مجسات الاهتزاز (Vibration) من مثل الصوتي (Acoustic) والزلزالي (Seismic)، أو مجسات الضغط يمكن أن تتحسس وتكشف حركة الآلات الكبيرة وبمجسات الجاذبية (Gravimtvic)، والمغناطيسية (Magnetic)، تميز الحافلات من خلال وزنها أو كمية

الفصل الحادي عشر

الاختراق

مقدمـة

إن الدخول غير المسموح به (من حيث الصلاحية، أو السلطة أو القانون) وبنية السلب (Defraud) أو الخرق(Trespass)، لحُرمة الحاسب لسرقة كلمات الدخول أو الرموز الأخرى جريمة يعاقب عليها القانون في كثير من الدول حالياً. وفيما يلي مجموعة من أشكال الخرق غير الشرعي للحاسب، وما يحصل عليه المتطفلون من الحصول على طريقة للدخول.

إن عملية خرق حرمة الحاسب والوصول إليه بطريقة غير قانونية ودون صلاحيات يشمل الوصول إلى حسابات على النظام. إن الدخول إلى تلك الحسابات من المتطفلين يمكنهم من الوصول إلى المعلومات (مثل الملفات، البرامج، البريد المرسل لحسابات أخرى أو القادم منها). وللعديد من أنظمة الحاسب ما يسمى الحساب المركزي، والوصول إلى هذا الحساب سواء كان على الوندوز، أو يونكس يمكن من الوصول إلى أي معلومة أو محتوى على النظام وخاصة البرمجيات ويُمكن من التغيير في البرامج والمسح والتعديل . . . إلخ. وغالباً ما يقوم القراصنة بتكوين حساباتهم على الحاسبات التي يخرقون حرمتها.

لقد قام نيكولاس ريان (Nicolas Ryan) من جامعة ييل (Yale) بكتابة برنامج خاص به يمكنه من الحصول على خدمة ا لإنترنت مجاناً ودون حتى دفع فاتورة الهاتف، وتمكن من الدخول إلى شكبة (AOL) وتوزيع البرنامج، ولقد تم استخدام البرنامج من قبل مئات الأشخاص وقد قدر الأشخاص المستخدمين بـ(2000) شخص يومياً، ولقد حكم عليه (2) سنة وسجن (مراقبة) و(6) أشهر إقامة جبرية وغرامة (62.000)دولار للشركة (Hilzenrath, 1997).

أما تقرير الـ (FBI) فيورد أن خسارة الاختراق الإلكترونية في الولايات المتحدة وحدها قد بلغت حوالي (10) مليار دولار. وقد سجل أكثر من (3800) محاولة دخول للشبكات غير الرسمية لوكالة الأمن القومي في وزارة الدفاع الأمريكية (Ehlers, 1999).

وفي عام (1997) قامت وزارة الدفاع الأمريكية بإجراء مناورة حرب معلومات باسم (المتلقي الشرعي) لفحص البناء التحتي المعلوماتي، وقد زودت الدخلاء بالمعدات القانونية لخرق الأنظمة، ولقد ذكر جيمس آدمز (Adms) عن هذه المناورة «لقد ركزت الحملة على ثلاثة مجالات هامة هي: البنية التحتية المعلوماتية وهي القيادة العسكرية، والقيادة السياسة، وفي كل من هذه المجالات توصل الدخلاء إلى الوصول إلى النظم المهمة وتعطيل نظام السيطرة الجوية والطاقة ومصافي البترول». وخلص إلى القول إن بيرل هاربر إلكترونية ممكنة (في إشارة إلى معركة بيرل هاربر التي خسر فيها الأمريكان خسارة كبيرة من اليابان) (Gertz, 1998).

إن أول ما يحتاج إليه المتطفل (Intruder) هو الوصول إلى الحاسب، أو الشبكة سواء من خلال الاتصال (Dial-in) أو الشبكة (Netowrk). وإذا كان النظام على الإنترنت فإن المتطفل بحاجة إلى معرفة اسم الخادم (Domain Name)، أو العنوان (IP)، وإن إحدى طرق خرق حرمة الحاسب أو الشبكة هي من خلال تلنت (Telinet)، وهو برنامج حاسب يمكن من الدخول للشبكة عن بعد. ويُمكن أن تكون عملية الدخول بطريقة متنوعة بمساعدة أدوات خاصة وبرمجيات، أو بالوصول إلى كلمة الدخول، أو حذف محتويات الحافظة (*.*de).

أدوات الحصول على الدخول غير المصرح به وأساليبها

1ـ ماسحات الشبكة (Network Scanners):

هناك ماسحات للشبكة الهدف منها مساعدة إدارة الشبكات في تنظيمها وحمايتها من التعرض لسوء الاستخدام أو التعديات، ومن هذه الماسحات ماسحة الإنترنت الأمنية (ISS) وإدارة التحليل الأمني لتدقيق الشبكات (Security Analysis Tool for Auditing Network (SATAN)). إلا أن هذه البرمجيات والأدوات يمكن أن تستخدم من المتطفلين لإيجاد ثغرة أو مكان للدخول غير المشروع للشبكة. ففي عام 1996م، استخدم فارمر (Famer) ماسحة (Satan) في دراسة مسحية لـ(1700) موقع على الشبكة، وهذه المواقع تدار من البنوك، وإتحادات بطاقات الائتمان، والوكالات الفدرالية والصحف، وبعض مؤسسات الأعمال دون دخول فعلي إلى أنظمتهم، لقد وجد أن أكثر من (60%) يمكن خرقها، أو تدميرها، وهناك (9-24%) يمكن أن تجتاح من القراصنة (Farmer, 1996).

2 ـ **رزم الشم**(Packet Sniffer)

لقد تم الكشف في عام (1993م) من قبل (CERT/CC) عن كشافة في التطفل على الإنترنت مختلفة عن الاعتداءات السابقة. حيث يدخل المتطفلون والقراصنة إلى الحسابات ويضعون رزم شمشمة المعلومات للحصول على الأسماء وكلمات الدخول، وأحياناً يدخلون إلى الأنظمة لمقدمي خدمة الإنترنت حيث يتم جمع معلومات (الأسماء وكلمات الدخول) للكثير من المستخدمين لهذه النظم. لقد وجد أحد المقدمين لهذه الخدمة ملف (600k) يشمل على أكثر من (20.000) اسم مستخدم تمت قرصنتهم، وكلمات دخولهم، حيث استخدمت هذه الأسماء لقرصنة المزيد من النظم وجمع المزيد من الأسماء (Denning & Denning, 1997) .

3ـ **مروّجو كلمات الدخول** (Password Crackers)

عادة ما تحفظ كلمات الدخول مشفرة في ملف خاص حيث تستخدم كلمة المرور (Password) كمفتاح لهذا التشفير، وإذا ما توصل القراصنة إلى هذا الملف فإنه يمكنهم فك تشفيره بواسطة بعض الأدوات مثل (Crack)، أو (LophtCrack)، وتقوم هذه البرامج بتتبع معجمي، حيث تتم متابعة كل كلمة وتستخدم كمفتاح في فك تشفير مجموعة (حزمة) من البيانات ومقارنة ذلك الكل المتكامل لكلمة الدخول، وإذا ما نجحت المقارنة (المطابقة) فإن الكلمة تكون هي كلمة الدخول لذلك الحاسب. ومن البرامج الفعالة في التقاط كلمات الدخول برنامج (LophtCrack)، وهذه الأداة تشتمل شمام الشبكة (Network Sniffer)، وبقدرة لـ(Crack) (10.000) كلمة دخول مرة واحدة، وله خاصية حفظ هذه المحاولات حيث يمكن استكمالها لاحقاً، ويعمل هذا البرنامج في الخلفية وبقدرة كاملة على الاختفاء وبمقدرة على إعادة الحفظ بمفتاح من المفاتيح الساخنة (.ctrl -alt -L) ، حيث يقوم الشمام بالتقاط الأسماء وكلمات السر من خلال الشبكة ومن ويندو (NT)، أو ويندوز (1995م).

4ـ **الهندسة الاجتماعية** (Social Engineering)

يستخدم قراصنة الحاسب انتحال شخصية أفراد مهمين، أو مهندس حاسب، أو فني حاسب . . . إلخ.، ويطلب المساعدة لدخول النظام، أو تأسيس حساب باسمه

. . . إلخ. وتشكل هذه الطريقة نسبة كبيرة في خرق أنظمة الحاسب. ومن الأمثلة الطريقة في هذا المجال أن أحد القراصنة تمكن من وضع إعلان على لوحة الشركة يعلن فيه أرقاماً جديدة للمساعدة، وقام الموظفون بالاتصال بالرقم وترك معلومات هامة تتعلق بالاسم، وكلمة المرور . . . إلخ.، حيث لم يكونوا يعلمون أنهم يتصلون بهاتف قرصان حاسب (Winkler, 1997). وهناك أدوات تساعد قراصنة الحاسب في الدخول إلى مزودي الخدمة وسرقة أرقام بطاقات الائتمان المستخدمة والأسماء، وكلمات المرور، ومن هذه البرامج برنامج (Aotlello)، وهو برنامج قرصنة تمكن من الدخول إلى شبكة (American online)، وسرقة معلومات مستخدمي هذه الشبكة. وأحياناً يحتال قراصنة الحاسب من خلال استخدام غرف الدردشة (Chat room)، ويختارون قوائم الأفراد ويتصلون بهم، وإفادتهم بأنهم «نحن من شركة . . . (الشركة المقدمة للخدمة) ولدينا صعوبات في تصليح بعض الملفات، لطفاً أكد لنا المعلومات الخاصة باسم المستخدم وكلمة المرور لنتمكن من تصويب الخطأ» (Tims, 2001).

5 ـ **سرقة المعلومات** (Information Theft)

عندما يتم خرق حرمة حساب الإنترنت، والدخول إلى الحاسبات،فإن المتطفل يتمكن من الدخول والوصول إلى المعلومات وقراءتها، أو تحميلها، والوصول لكل ما هو مسموح الوصول إليه لصاحب الحساب الأصلي بما في ذلك الوثائق الشخصية، والمؤسسية، والبريد، والوثائق الحساسة، وقواعد المعلومات.

6ـ **جمع التذكار** (Gathering Trophies): يعد التطفل على الإنترنت والقرصنة بالنسبة إلى المراهقين ليس بهدف جمع المال، أو تسبيب الأذى، ولكن للمتعة وجمع الأنصبة التذكارية (Trophies)، وهي الوثائق والشارة (Eidbits)، والتي يمكن التفاخر بها على خطوط الدردشة واللوحات الدعائية. ومن الأمثلة على مثل ذلك هو سرقة أرقام التشفير الخاصة بالفضائيات ومن ثم وضعها على البطاقة الخاصة بالمحطة المعنية.

كذلك فإن قراصنة الحاسب لا يخرقون حرمة الشبكة فقط، بل شركات التلفونات ويقومون بتنزيل برامج حساسة، ومعلومات هامة. ومن الأسماء المشهورة في هذا المجال هربرت زين (Herbert Zinn, Jr.) حيث دخل إلى العديد من قواعد المعلومات

والشبكات بما فيها (AT&T)، وسرقة برامج حساسة خاصة تتعلق بتصميم الحاسب والذكاء الصناعي وبرمجيات تستخدم من قبل شركات الهاتف في إرسال الفواتير للعملاء (Townson, 1989)، وكذلك كيفن متنيك (Kevin Mitnik) الذي قام خلال الثمانينات والتسعينات بخرق حرمة الكثير من الشبكات، وسرقة معلومات منها تقدر (160.000) دولار وبخسارة قدرت بـ(40.000) دولار (Hofner & Markoff, 1991).

والأمثلة على الدخول غير المشروع، أو السرقة للمعلومات، أو التخريب، أو الابتزاز بالمعلومات، أو سرقة بطاقات الائتمان، أو خدمات الهاتف كثيرة جداً، وقد تجاوزت التعديات هذه الفئات ليتمكن قراصنة الحاسب من الدخول إلى الأسرار الحكومية، وأعمال حتى اللجان مثل وزارة الخارجية السويسرية، وأعمال اللجان المعنية بتعويضات اليهود خلال الحرب العالمية الثانية، والدخول إلى وكالة الفضاء الأمريكية (NASA)، وسرقة البرنامج الذي صممته لكشف قراصنة الحاسب (Denning, 2000 b).

7 ـ **التأثير** (Tampering)

يحاول المتطفلون أن يأثروا في محتويات الحاسب الذي يخرقون حرمته حيث يقومون بتكوين حسابات شكلية (تقليدية) (Phony) لاستخدامها في عمليات الولوج للنظام وتثبيت برامج الشم (Sniffer) لالتقاط أسماء المستخدمين وكلمات دخولهم، ومسح مساراتهم من ملفات الدخول (Logon files)، ووضع برنامج أدوات مساعدة عادةً يخفي دخولهم إلى النظام ويساعد في عمليات القرصنة. والهدف من هذه العلميات تحطيم كامل النظام عامة والبيانات. ويحتاج صاحب النظام إلى وقت لإعادة النظام والبيانات إلى ما كانت عليه، مما يؤدي إلى تعطيل النظام لبعض الوقت. وهناك العديد من حالات الدخول غير المشروع لحسابات البنوك وتحويلها إلى حسابات شكلية، ومن ثم إلى حسابات أشخاص في دول أخرى، أو الدخول إلى الصحف وتعديل المقالات، أو تغيير علامات الطلاب.

8- **قرصنة المواقع على الشبكة** (Web Hacks):

تعد مواقع الشبكات من الأمكنة المفضلة للقراصنة، قد يكون ذلك بسبب تدني مستوى الأمن عليها والمستوى العالي من انكشافها. وهناك عدد من الحالات التي نجح

القراصنة فيها باجتياح المواقع الحكومية والمؤسسية وقاموا بتغييرات رئيسة فيها، ومن الأمثلة على هذه الأفعال في عام 1997 أحد المراهقين من ديلوقر (Delawgre) نجح في قرصنة موقع (NASA)، ووضع عبارات منها «نحن نملككم . . .»، وأن المسؤولين الذين يديرون هذا الموقع «أغبياء». أما صفحة موقع قسم العدالة فقد تم استبدالها بخلفية (Swastikas)، وبصورة ملونة لادلوف هتلر، وقد وضعت صورة المدعي العام مع صورة لإحدى نجوم التلفزيون عارية، ومع جُمل ضد الحكومة,Neil) (1997. وقد تم عنونة الصفحة باسم «قسم اللاعدالة الأميركي». أما صفحة وكالة المخابرات المركزية (CIA)، فقد غير اسم الصفحة إلى «أهلاً بكم في وكالة الغباء المركزية»، وقد تم ربطها بمواقع الصور الإباحية.

وفي عام 1998 (شهر حزيران) تمكن عدد من القراصنة يسمون أنفسهم (Milworm) من قرصنة مركز بحوث الذرة الهندية المعروف باسم India Bhabha) (Atomic Research Center [BARC] كإجراء ضد التجارب النووية الهندية في تلك الفترة، ولقد تمكنوا من السيطرة على (6 من 8) من خادمات الحاسب (Servers)، ولقد تمكنوا من تحميل آلاف الصفحات من البريد الإلكتروني والوثائق بما في ذلك مراسلات بين الباحثين الهنود والإسرائيلين، وقاموا بمسح المعلومات عن اثنين من الخادمات (Glave, 1998).

وتتركز غالبية حوادث قرصنة المواقع في الولايات المتحدة، وكندا، وألمانيا، وماليزيا، واليابان، واستراليا. أما الضحايا فهم في الغالب الحكومة الأمريكية، وقطاع الأعمال، والجامعات، والمواقع السياسية.

9ـ الغلق عن بعد (Remote Shutdown)

يمكن للمخربين وقراصنة الحاسب غلق خادم الحاسب عن بعد، حتى دون الحاجة إلى الدخول إلى نظامه. ومن الطرق المستخدمة والبسيطة ما أعلنه تود فاست Todd) (Fast على أنه يمكن أن يغلق أي خادم يستخدم ميكروسوفت (NT4.0) للإنترنت إصدار (3)، وكل ما عليه أن يفعله أن يطلب وثيقة (أي وثيقة) باسم طويل مما يؤدي إلى توقف الخادم مثل أن يدخل إلى خادم الإنترنت باسم (NAASS.COM) والطلب

(http://Naass.com/vrime=sssssssss، وعندما يتلقى الخادم الطلب، يحدث خرقاً للدخول ويتوقف الخادم (Fast, 1997).

وقد تتعثر بعض النظم وتتوقف من خلال استخدام خدع برنامج بنج (Ping) وهو الاسم المختصر لـ (Ping of Death)، وعادة يعمل برنامج بنج لتحديد الخادمات العاملة، الشبكة، حيث يرسل بروتوكولاً لضبط الرسالة (صدى) والمختصر (CIMP) إلى الخادم الهدف حيث يتستجيب إذا كان عاملاً، ويعمل برنامج البنج (Ping) من خلال إرسال رزمة أطول من (536،65) بايت (مقارنة في الرزمة التلقائية 64 بايت)، وعندما يتم تجميعها على الجهاز المعني (الهدف) قد تؤدي إلى توقف الجهاز أو انهيار النظام (Che, 1996). بالإضافة إلى ذلك هناك العديد من البرمجيات والأدوات التي تهدف إلى تعطيل عمل خادم الإنترنت.

التخريب (Sabotage)

إن أفعال التخريب (Sabotage) والتعدي على الممتلكات العامة (Vandalism)، وخاصة نظم الاتصال وخدمات الهاتف، والحرب الإلكترونية، والتعديات الفيزيقية كثيرة، وتشمل استخدام الأسلحة التقليدية لتدمير الأبنية الاتصالية أو تعطيلها أو إضعافها.

ومن الأدوات المستخدمة في هذا المجال:

1 ـ **التشويش** (Jamming): يستخدم التشويش في تداخل الموجات مع بعضها البعض مما يفشل عملية البث من المصدر المعني، وغالباً ما يستخدم التشويش في الراديو والتلفزيون. وعادة من السهل التشويش على الرادارات لأنها تعرف من خلال تردد واحد وعندما يعرف التردد فإنه يمكن التشويش على التردد بسهولة. أما الرادارات الحديثة فتنتقل من تردد إلى آخر، حيث لابد من معرفة تردداتها إذا رغب بالتشويش عليها، وتوجيه الإشارة الصادرة للتشويش بناءً على ذلك. ومع التقنيات الرقمية المضغوطة (Compression)، وتكرار الإشارات فإن الاتصالات في مأمن من التشويش. ويمكن التشويش على اتصالات الميكرويف، ففي عام (1997)م أعلنت الشركة الروسية ايفاكونفرسيا (Aviaconversia) عن مشوش (4وات) بأقل من (4.000) دولار يمكنه التشويش على إشارات الميكروويف الصادرة من النظام الدولي

لتحديد المواقع (GPS) على مسافة 200 كم (Radius). وقد يمكن هذا النظام أي دولة أو مجموعة إرهابية من تعطيل نظم الملاحة في الطائرات أو الصواريخ الموجهة بـ (GPS)، والنظم الأخرى التي تعتمد على (GPS).

وقد يؤدي مثل هذا التشويش على اطدام الطائرات، وتسخدم الحكومات التشويش لمراقبة البث المحلي، أو الخارجي والذي ينظر إليه على أنه غير مرغوب فيه لأسباب مختلفة وخاصة (الأمنية). وكانت الكثير من الحالات لاستخدام التشويش في حرب الخليج، والبلقان، والبوسنة . . . إلخ.

2 ـ **قنابل تحويل النضبات الكهرومامغناطيسية** (EMP/T) : تعمل قنابل تحويل النبضات الكهرومغناطيسية (Electromagnetic Pulse Transformer Bombs)، الطريقة نفسها التي تعمل بها بندقية الـ(HERF)، إلا إنها أكثر فعالية وقوة من منها، وأن التدمير الذي تحدثه يبقى مستديماً، وغير مؤقت كما هو الحال في بالنسبة لبنادق (HERF). ولقد أظهر تقرير وكالة إدارة الأزمة الفدرالية أن الأجهزة التالية من المرجح أن لا تعمل في حالة تعرفها إلى هذه القنابل، والحاسبات، والتيار الكهربائي للحاسبات، ومزودات الترانزستورات، ومكونات أشباه المواصلات تؤدي إلى إيقاف عمل الكوابل الكهربائية، ونظم الإنذار (Alarm Systems)، نظم الاتصالات المباشرة (Intercom Systems)، ومعدات التلفونات وترانزستورات الإرسال، والاستقبال، ونظم ضبط القوة والاتصالات.

3ـ **بنادق** (HERF): وهي بنادق ذات ترددات راديو عالية (Hig Energy Raidion Frequency) تؤدي إلى الحرمان من الخدمة (Denial-of-Service) للعديد من الخدمات، وهذا السلاح بسيط التركيب، ويعتمد على الحجم، وقوة المصدر المستخدم،والمدى أو الدقة المطلوبة. ويمكن تصميمها بأشكال وأنواع مختلفة، وتقوم البنادق بتوجيه إشارات الراديو العالية إلى هدف محدد مسبقاً.

والدوائر الكهربائية أكثر عرضة لأن تحمل حمولة زائدة (Overload)، وهذا ما يمكن استغلاله من هذه بندقية، وببساطة فإن هذه البنادق ما هي إلا مرسل راديو يشبه المرسلات المضيئة في أعلى الأبراج والتي تحذر الطائرات من الاصطدام بها، وتعمل العديد من التقنيات الحديثة مثل جهاز الحاسب المحمول (Portable)، أو الجوال (Cellularphone) بمستويات طاقة منخفضة. وتعمل من خلال التصويب على الهدف

وتحميله طاقة زائدة تؤدي إلى تعطيل إرساله. فمثلاً يمكن أن تعطل الحاسب، أو شبكة حاسبات، أو تلفون . . . إلخ. حيث إن هذه المعدات مصممة بمستويات طاقة متدنية (Low-level signale). وعندما يضاف إلى دوائرها (ما ترسله) حمولة زائدة لا تستطيع العمل، وبالتالي تتعطل، أو تتوقف مرحليا (Schwartau, 1994).

4 ـ **أسلحة ترددات الراديو** (Radio Frequency Weapons): أسلحة تردد الراديو هي معدات تهدف إلى إصدار الإشعاع الالكترومغناطيسي في مكان ما في مجال الراديو، وإعاقة أو تدمير المعدات الإلكترونية التي تصدر الإشعاع، والهدف قد يكون حاسباً، أو مستقبلاً إلكتروني، أو نظام ملاحة، أو نظام تحذير. وقد تكون الأسلحة ذات موجات واسعة، أو ضيقة. مباشرة، أو غير مباشرة، أحادية النبض أو متعددة أو متكررة أو مستمرة. والمعدات التي تصدر النبضات الواسعة تسمى أسلحة النبض الإلكترومغناطيسية (Electronmagnetic Pulse [EMP]). ترسل المعدات الخاصة بالموجات الواسعة (Broadband) مجالاً كهرومغناطيسياً حاداً يدور اثنين أو أكثر من عشرات الترددات والإرساليات من الموجات الكهرومغناطيسية يمكن أن تكون مباشرة، أو غير مباشرة ويمكن إصدارها مرة أو عدة مرات. والمجال المرسل عادة ما يكون عالي الفولتية (High-Voltage Spike) على الكوابل والأسلاك، مما يؤدي إلى تعطيل وتخريب الدوائر الكهربائية، والأدوات في هذه الفئة تشمل (EMP) الذرية.

في عام (1998)م تمت محاكمة ديفيد شرنر (David Schriner) مهندس في شركة متخصصة في حرب المعلومات ومتقاعد من مكان فحص أسلحة البحرية بأنه قد تمكن وبنجاح في حديقة منزله من بناء سلاح ذي موجة عامة (RF) بواسطة (Oil Spark-gap Switshes) مواد متاحة حصل عليها بالبريد لمواد كلفت (500) دولار، والوحدة التي أسماها معدة الإرسال الإلكترومغناطيسي (TED)، كانت جاهرة للفحص أسبوعين من بداية العمل فيها ولقد استخدم (Two ignition coils)، وبطارية للطاقة، ووقود سيارات يضخ ويصفي (oil circulation)، ومن الزيت المتوفر المتحول. إنها تولد أمواجاً من موجة (FM) إلى أمواج متدنية من الميكروويف، وإنها تمثل سلاحاً جذاباً للإرهاب حيث يمكن وضعها في شاحنة أو سيارة ووضعها في مواقف السيارات، أو في مواجهة الأبنية. والمعلومات التقنية لبنائها متوافرة من المصادر المتاحة (المفتوحة) (Schriner, 1988).

5- **أسلحة الموجات الضيقة** (Narrowband) (RF) تنتج حامل موجة تردد راديو، إما مستمرة أو موجبة ضمن إطار ضيق من التردد دون العشرة من التردد. ويمكن أن يكون ناقل الموجة (Very High Frequency [VHF])، أو (Ultrahigh Frequency [UHF])، أو لوحة ميكروويف. وتؤدي إلى أمواج ذات فولتية عالية مما يؤدي إلى تخريب مكونات أشباه الموصلات، أو تعطيل عملها. أسلحة (RF) ذات تأثير عال عندما تكون مباشرة. ومن الأسلحة الفاعلة في هذه الفئة الميكروويف ذو القوة العالية (HPM)، ومن التقارير حول استخدام أسلحة (RF) من قبل الإرهابيين والمجرمين ما ظهر في الصن دي تايمز (Sunday Times)، بتاريخ 2/ 6/ 1996م «بأن المدينة محاصرة إلى 400 مليون عصابة»، حيث إن المقالة تذكر أن المعهد المالي قد دفع كمية كبيرة من المال إلى المبتزين الذين يستخدمون أسلحة معلوماتية متقدمة، حيث تمكنوا من الدخول إلى أنظمة الحاسب باستخدام القنابل الذكية، والموجات الكهربائية وبنادق (HERF)، أو (High emission radio Frequency)، والتي تؤدي إلى عاصفة من "الرياح" الإلكترونية خلال نظم الحاسب، ويستخدم المجرمون في روسيا معدات ذات طاقة عالية لإيقاف لوقت معقول أجهزة الانذار، وهناك بندقية إلكترونية تضعف وتعجز الراديو المحولة والتلفونات الجوالة. ويستخدم الإرهابيون معدات إلكترومغناطيسية مثل أسلحة (RF) لمهاجمة نظم الإنذار أو المؤسسات المالية، ويمكن أن يعطلوا السيارات، فمثلاً يمكن لأسلحة (EMF)، أن تخرب السيارات على مسافة (30م) وتؤدي إلى إيقاف المحرك على مسافة 90 متراً (Hayward, 1997).

في عام 1985م هاجمت جماعة إرهابية تسمى جماعة العلاج الوسيط (Middle Care Factur) نظام القطاعات للمسافرين، مما أدى إلى فوضى خلال ساعات الذروة، وقد تم التشويش على ترددات راديو الإنقاذ والشرطة، وقد أثر التأخير في حوالي (6.5) مليون شخص وقدرت الخسارة بـ (6) مليون دولار (موثق في Denning, 1999, p 201).

الفصل الثاني عشر

التنكر والخفاء

مقدمـة

إن عمل حرب المعلومات عادة ما يكون من قبل المتنكرين والمختفين خلف الواجهة المحتالين (Imposters). والذين قد يقومون بسرقة الهويات لسحب النقود، أو أخذ القروض، أو استخدام البطاقات الإئتمانية في شراء السلع بأسماء الآخرين، أو تزوير المستندات (Forgerry)، وتزوير الرسائل الإلكترونية، والتزوير والتزييف (Counterfeiting)، واستخدام برامج حصن طروادة الفيروسية.

يتناول هذا الفصل عدداً من أشكال التنكر والخفاء والتعمية والتي تقوم على خداع الطرف الآخر وجعله يتقبل المعلومات الخاطئة أو المزيفة. وفيما يلي مجموعة من هذه الاشكال وهي:

أولاً: سرقة البطاقة (الهوية) (Identity Theft)

سرقة الهوية تعني سوء استخدام هوية شخص آخر من مثل استخدام اسمه، أو رقمه الوطني، أو رخصة القيادة، أو بطاقة الائتمان، أو أرقام حساباته. والهدف هو اتخاذ أفعال مسموح بها لحامل الهوية مثل السحب النقدي، أو تحويل مبالغ مالية، أو تسجيل مشتريات على بطاقة الائتمان... إلخ. ولا تتوقف الخسارة عند الجانب المادي، بل الجانب المعنوي من كشف حسابات ومعلومات تتعلق بالضحية، وتعد هذه الاشكال من المعلومات معلومات خصوصية عنه. وعادة ما تشمل سرقة الهوية الشخصية الاحتيال، وسوء استخدام بطاقات الائتمان المسروقة، ويقوم السارق بتزوير وتزييف البطاقات والأرقام لشراء السلع والمواد التي يرغبونها. ويمكنهم من الاحتيال حتى في استخدام البطاقات حيث يمكن تحرير شيكات ومن ثم سحب الرصيد قبل وصول الشيك للتحصيل. وفي تقرير صدر عام (1998م) عن (GAO) حول سرقة الهويات في الولايات المتحدة، بأنه قدرت الخسارة الناجمة عن سرقة الهويات والتي تمت معالجتها عن طريق مكتب الخدمات السرية قد ارتفع من (450) مليون دولار عام (1996) إلى (745) مليون دولار عام (1997). وأن ماستركارد وحده قد خسر (407) مليون دولار عام (1997) (GAO, 1998).

ومن السهولة بمكان الحصول على معلومات عن أي شخص إذا حصلت على رقمه الوطني، أو رقم يدل على شخصيته، وتكثر الجرائم الناجمة عن سرقة الهوية في مجال المال وبخاصة سرقة الحسابات من البنوك، ومن أجهزة الصرف الآلي، وقد يقوم بمثل هذه الأعمال موظفون من داخل البنك حيث يسرقون أرقام حسابات العملاء في مرحلة ما وبعدها يتركون البنك ليقوموا بسرقة حساباتهم لاحقاً. كما يمكن أن يقوموا بتحويل أجزاء بسيطة من آلاف الحسابات ويجمعونها في حساباتهم، بحيث لا يشعر أصحاب الحسابات الاصلية بهذا المبلغ، من مثل تحويل مبلغ دولار واحد من (10) آلاف حساب، من أصحاب الارصدة الكبيرة.

ثانياً: الرسائل والوثائق المزورة (Forged Documents and Messages)

التزوير سلوك من سلوكيات حرب المعلومات، والتحريف في الوثائق يهدد شخصية الوثيقة الأصلية، وتصبح قيمة الوثيقة عالية بالنسبة للمزور، ولكن قيمتها تهبط لدى الآخرين لمعرفتها باحتمال أن النسخة المتوافرة هي نسخة مزورة ولست الأصلية. والتزوير نوع من سرقة الهوية حيث يستخدم سارقو الهوية التزوير والتواقيع على الشيكات المسروقة، أو طلبات بطاقات الائتمان، أو أية وثيقة أخرى للضحية، ومن هذا المنظور فإن التزوير نوع من أنواع سرقة الهوية، وهي نوع من إدارة الإدراك يهدف خداع الآخرين باقناعهم بأن الوثيقة المزورة هي وثيقة أصلية.

لقد تبين أن جميع الوثائق التي تدعي أن جون أف كيندي (Kennedy) مرتبط بكل شيء من مارلين مونرو (Marilyn Monroe) إلى المافيا كلها وثائق مزورة، وهذا ما كشفه أحد خبراء التزوير لبرنامج (CBS) ستون دقيقة. ومع توافر الحاسبات فقد سهل عملية التزوير، حيث يمكن تكوين وثيقة جديدة، ووضع اسم أي شخص عليها. والبريد الإلكتروني يوفر طريقة فاعلة في الاحتيال.

1- تزوير البريد الإلكتروني (E-Mail Forgeries).

إحدى الطرق في تزوير البريد الإلكتروني هو خرق حرمة حساب الحاسب، وإرسال رسائل من داخل ذلك الحساب، ومن الأمثلة على مثل هذا الخرق ما تعرض له أحد الأساتذة في (Texas A&M)، حيث أرسل المتطفل من خلال حساب الأستاذ (20.000) عشرين ألف رسالة تعصب، وكنتيجة لذلك تلقى الأستاذ تهديدات بالموت

(Littleton, 1995). ومن الحالات الأخرى كذلك قيام إحدى موظفات شركة أوركل (Oracle) والتي اشتكت على الشركة مدعية أن مدير الشركة لاري إليسون (Larry Ellison) فصلها لأنها قطعت علاقتها (الجنسية) معه. ولكي تدعم أقوالها فقد قامت أدلين (Adelyn) بإنتاج رسائل إلكترونية من حساب مديرها الإلكتروني، يقول فيها إنه أنهى خدماتها بناءً على طلب إليسون، ولكن مديرها لم يكن قد أرسل هذه الرسائل، ولقد حكمت في عام (1997) في التزوير وانتحال صفة الغير، والكذب، وخرق حرمة الحاسب (Associated Press, 1997).

وليس المزور بحاجة إلى الدخول إلى حساب الشخص المعني لإرسال رسائل باسم شخص آخر، فمن السهولة بمكان أن يجهز عنوان البريد الصادر (Outgoing e-mial address) بأي اسم حتى لو كان البيت الأبيض الأمريكي، أو الرئيس الأمريكي (President@Whitehouse.gov) مما يجعل الرسائل الصادرة تبدو كما لو أرسلت من هذا العنوان. كما أن هناك العديد من البرامج التي تجمع عناوين الأشخاص من خادمات الحاسب وهي المعروفة بجامعة العناوين البريدية (E-mail collector) وبالتالي يمكن أن يمطر الشخص مئات والآلاف العناوين بما يريد أو أن يرسل لها ما يريد.

2ـ **التزوير في البريد الدعائي** (Forgeries in Spam)

بريد المهملات (Junk) أو بريد الدعايات غالباً ما يحمل معه عناوين مفخخة، أو ما تسمى (Bogus). وهناك مئات القضايا بين الشركات، أو الأفراد بسبب إرسال هذا النوع من الرسائل الهادفة إلى تعطيل أو تشويه سمعة شركة ما أو حرمانها من الخدمة لفترة، أو هدم مصداقيتها مع زبائنها.

3- **الفيضانات البريدية** (E-Mail Floods).

وتستخدم هذه الاستعارة للإشارة إلى آلاف الرسائل المفخخة إلكترونياً التي ترسل إلى بريد الضحية، أو بملف ملحق (Attachment) بحجم كبير جداً، وهذه ما تسمى أحياناً القنابل البريدية (E-mial Bombs) مما يحول دون وصول الرسائل القادمة لصندوق بريد الضحية، مما يؤدي إلى حرمانه من الخدمة أو نكرانها عليه، وغالباً ما يكون الدافع هو الانتقام أو التحرش. ومن الأساليب الأخرى في هذا النوع من

التعدي هو وضع اسم الضحية لدى آلاف المواقع من القوائم البريدية الإلكترونية، حيث يقوم كل موقع بإرسالها إلى زبائنه مما يعني تجميع مئات الآلاف من الرسائل في صندوق واحد هو صندوق الضحية. ولوقف الهجوم (الفيضان) على الضحية أن يرد برسالة يطلب فيها عدم رغبته بالاشتراك، وقد يكون المهاجم قد شغل برنامجاً خلفياً يقوم بإعادة الاشتراك لكل اشتراك مغلي. وقداستخدمت هذه الطريقة ضد الرئيس الأمريكي السابق بل كلينتون (Kornblum, 1997).

4- **تغيير العنوان** (IP Spoofing):

في إرسال الرسائل حقل هو المرسل (From) وحقل آخر المرسل إليه (To) وكل من هذين الحقلين يشمل على عنوان بروتوكول (Interent Protocol IP) الخاص بالحاسب على الإنترنت. ومن الهجمات الشائعة ما يسمى (IP Spoofing) وهو تزوير المرسل الحقيقي. إن معرفة عنوان البروتوكول للانترنت للخادم يمكن المتطفل من تخمين هذا العنوان للمشترك مثل :

10.0.0.103, 104,

والدخول إلى صاحب الحساب وإساءة استعماله.

5- **التزييف** (Counterfeiting)

التزييف أحد صيغ التزوير حيث يتم عمل وثائق هي في الأصل لمؤسسات أو وكالات حكومية. ومع توافر التقنيات الحديثة مثل الحاسب والطابعات، وامكانيات التعديل بالصور والخيالات ... إلخ. فإن الرموز والأساليب "الأختام" يمكن عملها بسهولة. وبالتالي يمكن تزوير وتزييف جوازات سفر، والأختام الحكومية، وصور وثائق ... إلخ (Denning, 2000 b).

وعادة فإن أية وثيقة مطبوعة مرشحة لأن تكون عرضة للتزييف بما في ذلك الرسائل، والتذاكر، وبطاقات الهوية، والعملات. وفي ولاية كارولاينا الجنوبية أطلق سراح شخص من السجون بناءً على فاكس أرسل باسم شريف الولاية من فاكس عام في محل لبيع الخضروات يطلب إطلاق سراحة (Neumann, 1997). وتعد العملة من المواضيع الشائع تزييفها، إن تزييف (5.000) ورقة نقدية من فئة (100) دولار تعني ثروة بالنسبة للمزيف وهو مبلغ كبير (500.000) دولار.

أوردت نيويورك تايمز (New York Times) أن حجم العملة الأمريكية (الدولار) المزيف في الفترة (1987ـ1996م). المصادرة في الولايات المتحدة وغيرها قد تضاعف من (89) مليون دولار إلى (205) مليون دولار، ثم إلى (339) مليون دولار عام 1995م. ولقد حدث أخيراً انخفاض بسبب الورقة النقدية الجديدة من فئة (100) دولار والإجراءات المضادة للتزييف، ويعتمد المزيفون على الحاسب في حوالي (82%) من مصادر التزييف لديهم مقارنة بـ (34%) قبل عشرة سنوات سابقة، و(90%) من الأوراق النقدية استخدمت فيها المطابع الكبرى.

وقد ساهم الحاسب في تسهيل عمليات التزييف حتى وصفت "التزييف نهاية الأسبوع" حيث إن غالبية النقود المزيفة من قبل مراهقين حتى أن أحداً منهم وضع صورته على الدولار بدل صورة فرانكلين، وتم القبض عليهم عندما حاول خاله استخدامها في الشراء من مطعم ماكدونالد (Johnson, 1997).

ثالثاً: حصن طروادة Trojan Horses

من المعروف عن القصة التاريخية عن حصن طروادة، حيث اختبأ الجنود اليونان داخل حصان خشبي، فعند دخولهم الى مدينة الاعداء وفتح البوابة الخشبة للحصن وهزموا أعدائهم. ويستخدم هذا المصطلح للدلالة على أي شيء يوضع داخل منطقة الخصم (حدوده) بطريقة تخفي طبيعة التخريبية (المدمرة). ويعد حصن طروادة أداة حرب المعلومات تستخدم للوصول للمعلومات ومصادرها.

1- **برمجيات حصن طروادة** (Software Trojans)

تشكل برمجيات حصن طروادة تهديداً لأمن المعلومات، حيث يمكنها أن تحذف ملفات، وتعيد تجهيز القرص الصلب، وإذا ما تم تشغيل الشيفرة (Code) فإن حصن طروادة تتحول إلى قنبلة منطقية (Logic bomb) أو إلى قنبلة وقت (time bomb). وهناك عدد من هذه البرمجيات منها على سبيل المثال: (Backorifice)، و (Bubble-Boy)، و(Irok)، و(Narnar)، و(QAZ.A)، (W32/Fix)، و(mypics)، و(Serbian)، و(Trinoo) .ويمكن زرع برنامج حصن طروادة في أي تطبيق من مثل ميكروسوفت وورد أو ألعاب الحاسب، أو أدوات النظام، ويمكن توزيعه من خلال البريد الالكتروني كملحق (attachment).

2- ركوب الوب (Riding the Web)

يوفر الوب (Web) أداة قوية في إرسال البرمجيات، وحصن طروادة ويمكن للمستخدم من تحميل (Download) برنامج كامل في الغالب مضغوط يمكن إعادته لوضعه بمجرد النقر على ايقونته. ومن القصص الطريفة في هذا المجال ما حدث في شهر (12) من عام (1996) لأحد المواقع المسماة (Sex girls.com) و(Ladult.com.) و(Beavisbutthead.com) حيث أعلم المتصفحون والزائرون أنه لكي يستطيعوا تصفح صور عارية فإنه يلزمهم برنامج خاص لاستعراض هذه الصور، ويمكن الحصول على هذا البرنامج من خلال النقر على رابط معين. وعندما يتم تنزيل هذا البرنامج والذي يحوي على فيروس من نوع حصن طروادة يقوم بايقاف المودم وإعادة تشغيله وربطه مع هاتف موجود في مولديفيا (Moldavia) (احدى المدن في الاتحاد السوفياتي السابق) ويجاب على الاتصال من خلال إعادته الربط بالموقع الأصلي (الموجود في كندا) ولكن المكالمة تدفع من مولديفيا وحتى عندما يوقف الحاسب عن العمل، فإن الفيروس يبقي الخط مفتوحا ويتم تسجيلها على المتصل (Fisher, 1997).

3- تتبع البريد الالكتروني E-mail Relays

عندما يترك الافراد مكان عملهم أو يغيرون بريدهم، فإنهم يضعون مكاناً يجمعون فيه كل حساباتهم البريدية، حيث تلحق بهم رسائلهم أينما كانوا، والمشكلة هنا هو أن البريد الالكتروني الذي يلحق بالفرد يمكن أن يكون مراقب من خلال الجهة التي تيعد إرساله إلى العنوان الجديد.

الفصل الثالث عشر

الوباء الإلكتروني

مقدمـة

الوباء الفضائي استعارة للمرض الوبائي (Epidemic)، وتعرف مثل هذه الأوبئة بأنها فتاكة بحياة الناس، وأنها تتوالد بكثرة وتقتل مقابلها في الحياة البيولوجية. أما في حرب المعلومات فالوباء الفضائي يعني البرامج التي تحاكي أسلوب حياة الناس، وهي مثل الوباء (Plague) معدية ويمكن أن تؤدي إلى خراب كبير. وبعضها يعمل كالقنابل يختفي حتى تتاح الفرصة له للانتشار، وحالما ينتشر في النظام يمكنها أن تخرب، وتعُطل النظام، ومن أهم الأوبئة الفضائية (الحاسوبية) فيروسات الحاسب (Computer Viruses)، والديدان (Worms).

الفيروسات (Viruses)

يعد فيروس الحاسب برنامجاً يقوم بتعديل البرامج الأخرى بحيث تقوم بتكرار (نسخ) الفيروس مرة أخرى (تكاثر). وهذه عملية مشابهة إلى عملية انتقال الفيروس الذي يصيب الإنسان.

في منتصف الثمانينات، وكما يقال فان «أمجد أخوان» كانا يديران محل حاسب في باكستان، ولقد أحبطا من قرصنة برمجيات الحاسب، فقاما بكتابة أول فيروس حاسب، وفيروس تشغيل أسماه العقل (Brain). ومن هذه البداية انتشرت الفيروسات. والفيروس جزء صغير، محتو ذاتي من رمز الحاسب مخفيّ داخل برنامج حاسب مثله مثل الفيروس الحقيقي. يمكن إعادة إنتاج نفسه وإصابة الحاسبات الأخرى وقد يختبئ أشهراً وسنوات قبل أن يهجم، إنه واحد من الأشياء التي تؤذي الحاسب، والديدان، والقنابل المنطقية، وحصن طروادة كلها أمثلة لمجموعة واحدة من فيروسات الحاسب.

وتنتشر فيروسات الحاسب بشكل كبير بسبب سهولة تكوينها، حيث لا يتطلب تكوينها معرفة كبيرة، فهناك حوالي (200-300) فيروس جديد كل شهر مع استمرار انتشار الأنواع القديمة. بالإضافة إلى زيادة انتشار الحاسبات الشخصية والمحمولة، والبريد الإلكتروني، والاتصال عن بعد، وزيادة الارتباط على الشبكات. وبناءً على تقرير نظم من الانترنت فإن هناك (71402) هجوم فيروس في الربع الأول من عام

(2000). ففى دراسة قامت بها مؤسسة ديتا كويست (Data Wuest) عام (1991) على المستخدمين للحاسب من الأمريكان والكنديين تبين أن الأقراص المصابة بالفيروس كانت مسؤولة عن نقل (87%) من الفيروصات، و(43%) من هذه الأقراص مسؤولة عن نقل الفيروسات إلى المؤسسات من خلال أقراص جلبت من المنزل. أما تحميل البرامج فكانت مسؤولةً عن (7%).

ولمواجهة الفيروسات فإن ذلك يتطلب أن تقوم الإدارة بتحميل البرامج بنفسها، ولا تسمح للموظفين بجلب الأقراص من منازلهم، أو وضع برامج عن طريقهم. وبعض المؤسسات تطلب فحص أي قرص يتم إحضاره من خارج المؤسسة. كما أن وضع برامج حماية ضد الفيروسات من الخطوات الهامة للتنبيه عن وجود فيروسات، وتنظيفها من الحاسب.

وفيروس الحاسب يدخل نسخة من نفسه في الرمز وعندما يتم تشغيل البرنامج يتم عمل نسخة من الفيروس، وهذا يحدث في نظام الحاسب، وإذا ما تم نقل برنامج (مصاب) بفيروس الحاسب فيمكن أن ينتقل معه الفيروس إلى نظام حاسب آخر، وبهذه الطريقة يلصق نفسه بتعليمات الحاسب بما في ذلك رموز التطبيقات، والرموز المستخدمة في تشغيل الحاسب وتعليمات الماكرو الموجودة في الوثيقة، وكلما يقوم المستخدم أو الحاسب بفعل ما يؤدي إلى تشغيله من مثل (إعادة تشغيل الحاسب، أو فتح البريد . . . إلخ). كما تلصق شيفرة (رموز) برموز الخادم بحيث يؤدي عمل البرنامج في الذاكرة إلى تشغيل الفيروس أولاً ويقوم الفيروس بالسيطرة على عمليات الضبط (التحكم) في الحاسب، وعندما يعمل الفيروس يقوم بزرع نسخة من نفسه في ذاكرة الحاسب، حيث تبقى "مقيمة" حتى غلق الحاسب. وتقوم النسخة المقيمة بملاحظة وتتبع الملفات غير المصابة وإصابتها، وتتباين شدة وخطورة الفيروسات من فيروس إلى آخر، فمثلاً فيروس (Win95/CIH) مدمر، فبالإضافة إلى مسحه لأول ميجابايت من المعلومات على القرص الصلب، فإنه يقوم بالكتابة على جزء من نظام الإدخال ـ الإخراج في الحاسب الآلي (Bios)، وحيث يحتاج الـ(Bios) لتشغيل الحاسب، فإنه من غير الممكن تشغيل الحاسب حتى بقرص تشغيل خارجي.

وتعود فكرة الإنتاج الذاتي للرمز (الشيفرة) (Self-reproducing code) إلى عام (1970) عندما استخدم بنفور (Benford) مصطلح فيروس للإشارة إلى رموز

الحاسب غير المرغوب فيه، والتي تنتج ذاتياً في الحاسبات. ولم يتسخدم هذا المصطلح بشكل رسمي إلا في الثمانينات من قبل فرد كون (Fred Cohen) (Denning, 2000 b).

لقد عُرف فيروس الحاسب بأنه «برنامج يمكن أن يصيب» برامج أخرى من خلال تعديلها لتشمل نسخة منه ومن خلال المواد المصابة يمكن للفيروس الانتشار خلال نظام الحاسب، أو الشبكة مستخدماً صلاحيات كل مستخدم لإصابة برامجه، وكل برنامج يصاب يمكن أن يعمل كفيروس وتزداد الإصابات.

ومع بداية عام (1988) كان هناك (13) ألف فيروس حاسب ويمكن للفيروس أن ينتقل إلى البرامج والوثائق من خلال الأقراص المرنة، والمدمجة، والملحقات الإلكترونية.

تحدث التعديات الفضائية من أي مكان من العالم، فلقد تمكن طالبان فلبينيان من وضع فيروس سمي (I - Love -you). وتسبب ذلك في خسارة ملايين الدولات من جراء إغلاق نظم الحاسبات وحرمان مستخدميها من الخدمة جراء ذلك.(Borchgrave et. al., 2000).

1- **فيروسات قطاع التشغيل** (Boot Sector).

إن الجزء الخاص بتشغيل النظام هو أول جزء يُحمل على الحاسب وهذا البرنامج موجود على القرص وهذا قد يكون قرصاً خارجياً أو القرص الصلب في الحاسب أو قرصاً مدمجاً. وعند تشغيل الحاسب فإن المعدات تلقائياً تبحث عن هذا الجزء من البرنامج، وبالتالي فهو يقود إلى نظام التشغيل في الذاكرة، وبدونه فإن الحاسب لا يشغل البرنامج. ويقوم هذا الفيروس بتعديل برنامج قطاع التشغيل، وفي الغالب يصيب الحاسب إذا كان نظام التشغيل أصلاً مصاباً بالفيروس (قرص خارجي)، ومن أمثلة فيروسات قطاع التشغيل (Parity Boot) وهذا الفيروس يعرض الرسالة التالية (Parity Check) وبعدها يتحملها (يتوقف) نظام التشغيل، وهذه الرسالة مؤخوذة من الرسالة الخطأ التي يعرضها الحاسب عندما يكون هناك خطأ في الذاكرة. وبالتالي من يصاب حاسبه بهذا الفيروس يعتقد أن هناك خطأ في الذاكرة وليس فيروساً.

2ـ **فيروسات الماكرو** (Macro Virues).

فيروس الماكرو هو تعليمات يحملها برنامج تنفذ تلقائياً وغالبية البرامج (الوورد، والأكسل . . . إلخ.) التي تستخدم الماكرو. فيروس الماكرو ينتج نفسه بنفسه في كل مرة يشغل فيها البرنامج المصاب، وغالباً ما ينسخ الفيروس نفسه في ملف تشغيل البرنامج، وبالتالي فإن أية وثيقة تستخدم من خلال ذلك البرنامج تصبح مصابة. وإذا ما تم إرسال أية وثيقة سواء كانت على قرص أو بالبريد الإلكتروني فإنها تصيب برامج الشخص المتلقي لها. وهذه الفيروسات من أكثر أنواع الفيروسات انتشاراً، ولم تظهر فيروسات الماكرو إلا في منتصف عام (1995م).

3ـ **الفيروسات الطفيلية أو فيروسات التنفيذ** (Parasitic Viruses).

وهي فيروسات تلصق نفسها بالبرامج وتسمى أحياناً فيروسات التنفيذ (Executables) وعندما يقوم المستخدم بتشغيل البرنامج المصاب بهذا الفيروس فإن الفيروس يشتغل أولاً، وبشكل سري ويخفي وجوده عن المستخدم وبعدها يوعز للبرنامج الأصلي بالتشغيل ويصبح معلوماً لدى نظام التشغيل على أنه جزء منه ويعطيه كل الميزات المتاحة له، وهذه الميزات تمكن الفيروس من إعادة انتاج نفسه (نسخ) في الذاكرة، أو إعادة تحميله، فقط زيادة الحمل يمكن تلفت نظر المستخدم له. ومن الفيروسات المشهورة فيروس القدس الذي يبطئ النظام، ويمسح كل برنامج يشغله المستخدم. وعامة فإن نسبة انتشار فيروسات الماكرو (64%) والتشغيل (23%)، والطفيلية (13%) (Thenault, 1999).

4ـ **فيروسات البرنامج** (Program Viruses)

تلوث فيروسات البرنامج ملفات تحوي على شيفرة الحاسب خاصة ملفات (.EXE)، (.Com)، فكلما شغل المستخدم برنامجاً يحوي على ملف مصاب (Infected) يعمل الفيروس وينتشر.

الديدان (Worms).

تختلف الديدان عن الفيروس، حيث إنه برنامج مستقل ولا يعتمد على البرامج الأخرى، ولكي يعمل لا يحتاج إلى البرامج الأخرى، وهو يكرر نفسه (نسخ) على الحاسب ذاته، ويحاول أن يصيب الحاسبات الأخرى التي يمكن أن تكون متصلة

بالشبكة، وتقوم الفيروسات، والديدان (Worms) بهدم نظام الحاسب وتعطيله، وتدمير البيانات، وذلك في وقت معين، أو بعد تكاثر معين من النسخ. وقد تكون مخصصة لبرنامج تطبيقي معين، أو بيانات معينة. وقد تؤدي إلى خطورة كبيرة إذا أصابت حاسبات أنظمة الدفاع، مما قد يؤثر على برمجيات نظم الأسلحة . . . إلخ.

اقترح تحالف برمجيات الأعمال (Business Software Alliance) **المعايير التالية ضد الفيروسات:**

1- شراء واستخدام برمجيات زصلية.

2- وضع إرشادات ومراقبة للبرمجيات الجديدة.

3- التعلم بخطورة الفيروسات للمستخدمين.

4- عمل نسخ احتياطية للمعلومات والبرامج.

5- مراقبة الاتصال بالحاسب الخادم والشبكة.

6- مراقبة حقوق البرمجيات الممنوحة للمستخدمين.

7- تنظيف الحاسب من الفيروسات.

8- توفير نظم إدارية إضافية (Business Software Alliance).

ديدان الإنترنت (Internet Worms).

لقد انتشرت ديدان الإنترنت بسرعة، حيث تصيب النظام وبعد إصابة النظام تبحث عن سجل العناوين والبريد وترسل نفسها إلى كل من في سجل العناوين الخاص بالبريد. وديدان مثل (W22/Ska) (Happy 99) تعتمد على نظام ارسال البريد لتكاثرها، وتصل من خلال الملحقات عندما تستعمل من المستخدم.

حصن طروادة (Trojan Horse).

ملوثات تظهر مثل البرامج العادية وتنتظر لحين حدوث حادث ما أو تاريخ معين. . . . . لتدمر البيانات والملفات.

ومن أخطر هذه الأنواع حصن طروادة لأنها تمكن من الولوج إلى النظام عن بعد دون علمك عندما تكون على الإنترنت وعندما تُحمل برنامج من حصن طروادة فإنه

يمكن من السيطرة على ذلك الحاسب، فمثلاً يمكنك من جعل صينية الـ (CD) تفتح وتغلق مراراً دون إظهار سبب لذلك، ويمكن للشخص أن يقرأ، ويغير وينسخ ملفات الشخص الآخر دون علمه.

القنبلة المنطقية (Logic bomb)

برامج عادة ما تكون مخفية بعمق في الحاسب الرئيس ومخفية لتعمل في وقت ما في المستقبل لتدمير البيانات. إن الفرق بين فيروس الحاسب وغيره هو أن الفيروس قادر على إعادة انتاج نفسه بطريقة ذاتية، ودون علم المستخدم، ويحتوي على معلومات يعاد تحميلها (Payloads) مثل إعادة عبارة، أو رسائل مثل «أعتقد أن اسم المستخدم . . .».

ويمكن أن يكون مختفياً في برامج على أقراص مرنة، أو مدمجة، أو مصلقات البريد الإلكتروني (Theriauult, 1999). أما أكثر أنواع الفيروسات انتشاراً فهي فيروسات الماكرو(Macro)، والتشغيل (Boot)، والتنفيذ (Parasitic or Executables).

الجزء الرابع:

حرب المعلومات الدفاعية

- ◻ الفصل الرابع عشر : سد الثغرات والانكشافات
- ◻ الفصل الخامس عشر : مخابئ المعلومات
- ◻ الفصل السادس عشر : موثوقية المعلومات وأصالتها
- ◻ الفصل السابع عشر : حراسة المعلومات ورقابتها

تمهيد

يتناول هذا الجزء وسائل حرب المعلومات الدفاعية التي تُمكن من حماية المعلومات الحساسة المرتبطة بالبناء التحتي المعلوماتي الحساس للمجتمع عامة، وتصون المعلومات وتبقيها بعيدة عن التهديد من عمليات حرب المعلومات الهجومية. ويمكن أن تشكل الانكشافات (الفيريقية والفضائية) والممارسات الإنسانية، والثغرات تهديداً لأمن المعلومات، وحتى وسائل الدفاع قد تشمل مثل هذه الثغرات (التشفير، وجدران الحماية . . . إلخ.)كما يُعني هذا الجزء سد الثغرات في البناء التحتي المعلوماتي (الوقاية)، والإنذار المبكر، وتحديد التحديات، ومنع وقوعها على المعلومات. كما يتناول مخابئ المعلومات بما تشمله من حماية مادية للمعلومات ومعداتها، والتشفير والتخفية والإخفاء، واللامعلومية (المجهولية)، والترشيح والتخلص من نفايات المعلومات والتغطية المعلوماتية.

إن مفهوم حرب المعلومات الدفاعية (Defensive Information Warfare) يستخدم في الإشارة إلى «جميع الأفعال التي تهدف إلى الدفاع ضد الهجمات الموجهة للمعلومات، وهي هجمات على صناع القرار والمعلومات وعلى العمليات ذات الأساس المعلوماتي التي يعتمدون عليها، وعلى وسائل الاتصال الخاصة بقراراتهم، ويمكن أن تشن هذه الهجمات في أوقات الحرب وأوقات السلام، ومن قبل جماعات عسكرية أو مدنية» (Alberts, 1996, p. 2).

إن الدفاع ضد الهجمات على المعلومات ذو عدد من الخصائص المشابهة إلى الجهود الاجتماعية في مكافحة المرض، والمخدرات، والجريمة. ومن عناصر التشابه :

1ـ إن الحلول لمواجهة هذه المشكلات تتطلب جهوداً من عدد من المنظمات في القطاع العام والقطاع الخاص، و(التطوعي) ومنظمات المجتمع المدني.

2- إنه من الصعب وجود دعم كامل لأي من هذه الجهود.

3- إن هذه المشكلات ليست مشكلات جامدة (عصابات المخدرات تتعلم من أخطائها وتوظف تقنيات عالية في أعمالها) حتى الفيروسات (تتعلم) وتضعف مقاومة الجسم لها بعد أن تحصن نفسها ضد المحصنات الإنسانية.

4ـ الوعي العام مهم في المكافحة ويدعم المواجهة في مراحل معينة بعدها قد يخبو هذا الدعم.

5ـ المنظمات والأفراد يتعلمون التأقلم في سلوكهم في التعامل مع هجمات حرب المعلومات ومع النتائج غير المقصودة (Alberts, 1996)

ويشكل سد الثغرات والانكاشافات في البنية التحتية المعلوماتية الوطنية هدفاً استراتيجياً وطنياً تسعى الدول إلى تحقيق حماية للأمن الوطني وصيانة له. وتتركز حماية البناء التحتي المعلوماتي على عدة جوانب أهمها وضع المعلومات التي تحول دون وصول الأعداء أو المخربين إلى مكونات البناء التحتي والعبث بها أو تدميرها، والحيلولة دون الوصول إلى البناء التحتي المعلوماتي، ومراقبة البناء التحتي، وعدم السماح لمن ليس له حق الدخول في الوصول إلى نظم المعلومات ومكونات البناء التحتي.

كما يتم التركيز على التعليم الفني للموظفين والذين يمكنهم من التعامل مع أية خروقات للبناء التحتي ومعالجتها فوراً قبل استفحالها وتكوين ثقافة داعمة لأمن البناء التحتي لدى الفاعلين فيه. كما يجب الانتباه إلى الموظفين الذين لديهم حق الوصول إلى نظم المعلومات.

وفي مجال العمليات الأمنية يتم التركيز على توافر المعلومات ووضعها في أمكنة غير متاحة للمعتدين وخاصة إذا كانت هذه المعلومات مهمة وحساسة، والاحتفاظ بإمكانية شفاء المعلومات من أية كارثة قد تلحق بها كالحرائق، والسرقات، أو التدمير، ووضع الطرق الكفيلة بإيجاد البدائل (النسخ الاحتياطية). ويمكن الاعتماد على ما يسمى الروح الأمنية (Security Ethos).

أما في مجال الاتصالات فيمكن وضع جدران الحماية، والجدران (السياج) والأمن الشخصي (الشرطة) على المباني المهمة وخاصة المعلوماتية، ومراقبة حركة المعلومات من النظم وحمايتها إلكترونياً من الاقتراحات بالبرمجيات المناسبة. والاعتماد على آليات المنع والاعتراض للدخلاء على نظام المعلومات أو المتطفلين . . إلخ. كما ويمكن استخدام التشفير الذي يمكن من حماية إرسال البيانات وضمان مصداقيتها عند وصولها إلى الطرف المعني.

أما في مجال السياسات العامة، فلابد من وضع التشريعات المناسبة التي تعاقب المعتدين على المعلومات عامة سواء من الداخل أو الخارج، وحماية الثروة المعلوماتية وتفعيل وإنفاذ القوانين والأنظمة الخاصة بذلك. كما أن المنظمات المعلوماتية بحاجة إلى تقييم مستمر لوضعها الأمني ومعرفة الثغرات إن وجدت، ومعالجتها ويمكن استخدام أساليب التعديات الوهمية (المناورات الالكترونية) لمعالجة أية تعديات حقيقية أو وضع تجارب معينة لمعرفة مدى حصانة النظم المعلوماتية ضد الاختراقات.

وفي مجال التحقيق في التعديات لابد من حفظ الأدلة بحصول الاختراق والنظر إلى الموضوع بشكل تكاملي مع تجنب إلحاق أذى بالنظم التي لحق بها الأذى أصلاً ، أو إذا كانت عرضة للهجوم المعلوماتي، ولابد من تحديد هوية الفاعل أو المعتدي وتحديد المعلومات (الضحية).

الفصل الرابع عشر

سد الثغرات والانكشافات

مقدمة

يتناول هذا الفصل وسائل حماية سد الثغرات والانكاشافات، وخاصة المتعلقة بالبناء المعلوماتي الحساس، وخاصة مع تزايد الاعتمادية على المعلومات في كافة نشاطات الحياة الاجتماعية من البريد الإلكتروني إلى التحويلات المالية المحلية والدولية، وإلى الأسلحة والطيران، والكهرباء، والطاقة، والمياه، والخدمات الحكومية.

إن تعرض البناء التحتي لعدوان معلوماتي من شأنه أن يحول المجتمع والفرد في ظلام ليس متعلقاً بالاضاءة والرؤية، وإنما في السمع (الاتصالات)، والرؤية (الرادارات)، والطيران وكافة النشاطات الأخرى. لقد تنبهت الكثير من الدول مثل الولايات المتحدة الأمريكية وبريطانيا، وكندا، وفرنسا إلى مدى انكشاف البناء المعلوماتي التحتي وإيجاد السبل ووضع الاستراتيجيات اللازمة لحماية البناء المعلوماتي الحساس.

إن زيادة الاعتمادية على المعلومات، والترابط الوطني والدولي للأفراد والمؤسسات والمجتمعات (البناء المعلوماتي التحتي الكوني)، وسهولة الاختراق للبناء المعلوماتي وخطورة المعلومات خاصة إذا ما استغلت أو خربت، أو دمرت، جعلت الكثير من الدول تعطي موضوع حماية البناء المعلوماتي التحتي أهمية خاصة.

مراقبة الانكشافات (Vulnerabilities Monitoring)

تهدف مراقبة الانكشاف إلى تحديد الثغرات الأمنية في نظم المعلومات، وتشمل البناء الفيزيقي، والأقفال، وجدران الحماية، والمباني، والسلامة العامة، وأجهزة الحاسب، وكلمات الدخول . . . إلخ. إن المراقبة التقليدية (Surveillance) يمكن أن تكشف المواد الدقيقة المهربة من الموقع، ويمكن لإجراءات التعامل مع المعلومات المكتوبة أن تحدد الممارسات الخطرة مثل أخذ الوثائق الحساسة إلى المنزل، ترك الحاسب مع الأوراق في الفندق، السماح للزوار التجول في المناطق الحساسة.

إن التدقيق في تاريخ الموظفين عملية هامة وتساعد في الاختيار المناسب للموظفين الجيدين، فمثلاً شركة صن للنظم الدقيقة (Sun Microsystems) تقبل فقط (9%) من طلبات المتقدمين لها بعد عملية المسح لتاريخهم، وترفض غالبية هذه الطلبات بسبب الكذب فيما يخص التاريخ الجرمي، أو التزوير في المعلومات المقدمة . . . إلخ.

إن أكثر تعرض يمكن أن يهدد أمن المعلومات هو الناس (People)، بعض الناس غير المدربين قد يقومون بتدمير الكثير من المعلومات أو العبث بأنظمة التشغيل وتعطيلها والبعض الأخر قد يقوم بمثل هذه الأفعال بقصد وعن سابق معرفة بما ستؤول إليه الحال، والبعض الآخر فقد امتهن الجريمة في التعدي على الحاسب وبرامجه والمعلومات التي يحملها.

أمن الأفراد موضوع عام يشمل أكثر من الوقاية من جرائم المعلومات، فغالبية جرائم المعلومات ترتكب من قبل الموظفين وإن كانوا مدفوعين بأسباب مختلفة. وبما أن الحاسب تمثل طريقة كمهاجمة الموقع عن بعد، فإن برامج حماية أمن الأفراد تتطلب أخذ هذا البعد بالحسبان. إن الطريقة التي تبعد الأفراد غير المسموح لهم قانونيا بدخول النظام تتطلب ابقاؤهم بعيداً عن نظام الحاسب، ومن ثم تحصين نظام الاتصالات بحيث يتطلب وقتاً طويلاً في الدخول للنظام عن بعد. ومن ثم النظر إلى الموظفين وتدقيق مؤهلاتهم وخبراتهم وملفاتهم قبل تعيينهم.

أنواع التهديدات: إن نوع التهديد الذي يمكن أن يشكله أي فرد إلى نظام المعلومات يعتمد على عدة عوامل منها :

1- نوع الدخول (Type of Access).

2- مستوى الخبرة (Level of Expertise).

3-الدافعية (Motivation).

1- **نوع الدخول**: إن مقدار التخريب والتدمير الذي يمكن أن يلحق بنظام المعلومات يعتمد وبدرجة كبيرة على مستوى الدخول (Access). فإذا كان لدى الفرد ميزات دخول فقط للشاشة، يختلف عن مقدار التخريب الممكن أن يحدث فيما لو كان لديه ميزات دخول لغرفة الحاسب، أو فيما لو كان الدخول عن بعد. ويعتمد الدخول على نوعية الشخص فالمستخدم أو العابث أو المبرمج أو الموظف كل واحد من

هذه الفئات لديه اهتمامات خاصة وبحاجة لنوعية دخول مختلف عن الآخر. وهنا لابد من تحديد الأشخاص ونوعية الدخول لكل منهم، وأن تكون ميزات الدخول بمقدار الحاجة، أما كما تسمى بالجيش المعرفة اللازمة فقط (Need to Know).

2- **مستوى الخبرة** : كلما زادت خبرة الشخص كلما زادت نوعية التهديدات التي يمكن أن يشكلها للحاسب، فبرمجة فيروس حاسب تتطلب معرفة متقدمة بالبرمجة، وقد يكون محلل النظم أو المبرمج قادراً على وضع برنامج فيروس يدمر النظام كلياً بعد فترة محددة في المستقبل.

3- **الدافعية** : إن تحديد دافعية الفرد الذي يرتكب جريمة الحاسب أو الذي يمكن أن يرتكب جريمة الحاسب عملية مهمة، فالموظف الذي يحب عمله أو يلاقي تقديراً من رئيسه فمن المستبعد أن يرتكب أية أعمال تعد أو تخريب في عمله.

وهناك عدة فئات من الأفراد، منهم الموظفون عامة، ويمكن أن يكون للموظفين العاملين علاقات بالفئات التالية تشكل تهديدات مختلفة للحاسب منها :

1-المتعاقدون والموردون (Venders and Contractors).

2- المجرمون (Criminals).

3- المخربون (Espionage agents).

أفاد إحصاء قام به اتحاد الإدارة الأمريكي أن (35%) من الشركات، و(81%) من الشركات المالية يقومون بمراقبة موظفيهم بتسجيل محادثاتهم الهاتفية وبريدهم الصوتي، والبحث في ملفاتهم في الكمبيوتر، وتصويرهم أثناء أداء أعمالهم. ومن هؤلاء يقوم (23%) بذلك بدون علم موظفيهم، ويقوم (37%) بمراقبة الأرقام المتصل عليها، وطول كل محادثة، و(10%) يسجلون هذه المحادثات، و(16%) يراقبون شاشات الموظفين، و(15%) يخزنون، ويراجعون البريد الإلكتروني.

إيجاد الثغرات في الحاسب والشبكات

في الفضاء المعلوماتي، فإن مراقبة الانكشاف تبدأ بتثبيت البرنامج. إن تشغيل برنامج النظام مباشرة من الصندوق فيه دعوة للمتطفلين، حيث ترسل الرزمة مع المواصفات الأولية لتثبت ذلك النظام، وهي مفتوحة بشكل واسع للتعدي. إن نظام التشغيل المستخدم لدعم خادم الشبكة ربما يأتي بكلمات دخول أولية (Default)، وهي

بسيطة بالنسبة لأي هاو لتخمينها، أو لأي شخص له صله بالنظام يمكنه الوصول للملف القابل للكتابة والقراءة .

إن التأكد من انكشافات البرنامج ومشكلات المواصفات يمكن أن تكشف وتحل قبل تشغيل النظام، وحتى بعد التثبيت فإنه من الضروري استمرار تحديث المراقبة، وإعادة المواصفات عند إضافة عنصر جديد، أو حذف عنصر قديم. إن إضافة خط الوصل بالانترنت، أو بواسطة الاتصال عن بعد ذو مضامين أمنية هامة. وهناك العديد من البرامج المجانية التي تساعد على تحديد نقاط الضعف والفجوات من مثل برنامج (Computer Oracle & Passward System [CIOS])، برنامج (Security Analysis Tool for Anditing Networks [SATAN]).

لقد أجرت وزارة الدفاع تجارب لفحص الثغرات الأمنية في حاسباتها حيث قامت وكالة نظم المعلومات الدفاعية (DISA) بـ(38) ألف هجوم على حاسبات الوزارة، حيث نجحت في الدخول من الباب الخلفي في (4,4%) من الحالات، وفي حالات إقامة علاقة (ثقة) في (65% -88%) من الـ (4%) (أي حوالي1% من حالات الاختراق) قد تقدمت بتقارير للجهات الأمنية المعنية (GAO, 1996).

كما قامت وكالة الأمن القومي بعملية تدريبية لمعرفة الثغرات والانكشافات في حاسبات الجيش الأمريكي، وقد عرفت مثل هذه المناورات بالمتلقي الشرعي (Eligible Receiver)، وقد تم استخدام أدوات متاحة على الشبكة في عمليات الاختراق والمراقبة ولقد تمكن الدخلاء من الحصول على ميزات للدخول على العديد من النظم العسكرية.

مراقبة المنشورات الأمنية

يمكن لإدارة النظم البقاء على اطلاع بأحدث ما يصدر في مجالات الانكشافات واحتماليات التعرض والحلول، والتهديدات من خلال المواكبة الدائمة للنشر العلمي في المجال الأمني، ومن المنظمات المهتمة بذلك مركز التنسيق لفريق الاستجابة لطوارئ الحاسب (CERT) و(SANS). وهناك العديد من المواقع على الانترنت والتي تزود الراغبين بكل جديد في مجال الثغرات، والفيروسات . . .الخ.

بناء النظم الآمنة

بدأ الاهتمام في الأجهزة الأمنية بشراء الأجهزة والبرمجيات التي تحقق أكبر قدر من الأمن للمعلومات السرية. لقد قامت وزارة الدفاع الأمريكية بعدة دراسات ولقاءات ومشاريع ففي عام (1981) نجم عنها إنشاء مركز أمن الحاسب الوطني (NCSC) التابع لوكالة الأمن القومي (NSA)، وكان أحد مشاريعهم بناء معايير موثوقة لتقييم النظم (TCSEC) الوثيقة التي عرفت فيما بعد بالكتاب البرتقالي (Orange Book) بسبب لون الغطاء الخارجي له، ولقد وضعت المعايير لتلبي ثلاثة أهداف :

1ـ لتقديم خطوط عامة للمصانع بخصوص الخصائص الأمنية اللازم بناؤها في نظمهم الحالية والمستقبلية مع الاهتمام الخاص بحماية البيانات السرية وعدم الكشف غير القانوني لها.

2ـ تقديم لوزارة الدفاع مقاييس لتقييم درجة الموثوقية الممكن وضعها في نظم المعلومات للبيانات السرية والمعلومات الحاساسة.

3ـ تقديم أسس لتحديد المتطلبات الأمنية، حيث حدد (TCSEC) نوعان من المتطلبات: الخصائص الأمنية الواجب توافرها والضمانات اللازم تلبيتها. ولقد قسمت المعاايير إلى أربعة مستويات (A, B, C, D) حيث يمثل (A) الأمن الشامل، وتمثل (D) لا أمن، وقد تم تقسيم (A,B,C) لتعطي (7) مستويات من الثقة. وقد بنت المعايير على مفهوم قاعدة الحاسب الموثوق (TCB) والتي تمثل المكونات الأمنية في النظام، وهي على النحو التالي من الأقل إلى الأكثر ثقة:

D ـ حماية دنيا (لا متطلبات).

C1 ـ الحماية الأمنية الحذرة، يجب أن تكون النظم قادرة على ضبط الدخول على أساس الفرد المستخدم ويجب فحصها لتحديد التغيرات في الدخول.

C2 ـ حماية ضبط الدخول، يجب أن توفر النظم المسؤولية الفردية من خلال إجراءات الدخول، والحركات، ويجب أن تشمل اختيارات الانكشاف التغيرات التي تخرق، أو تسمح بالدخول غير المصرح به للبيانات والسجلات الخاصة بالمستخدمين.

إدارة الخطورة (Risk Management)

تشمل إدارة الخطورة تحليل الخطورة وتحديد التهديدات، وتقدير الخطورة.

1ـ تحليل الخطورة (Risk Analysis)

عند الحديث عن وقاية المعلومات، لا بد من تحدد الخطورة التي تهدد المعلومات وأنظمتها ومعداتها، وتطبيق إجراءات أمن متنوعة لحماية هذه النظم. أن عملية أمن المعلومات عملية مقايضة، فبعض الشركات والمنظمات تنفق ما يناسب حماية أجهزتها جميع ضد الأخطار بعضها بمقدار الخسارة الناجمة عن الحماية. وهذه عملية تدعى تحليل الخطورة.

إن عملية تحليل الخطورة تتضمن طرح أسئلة تتعلق بالتهديدات (المخاوف) والانكشافات والإجراءات الاحترازية، وفيما يلي بعض هذه الأسئلة :

1ـ من الشخص الأكثر احتمالية بالاعتداء على نظام معلوماتك، ولماذا ؟

2ـ ما الذي يمكن أن يجده (معلومات، مال . . . إلخ.) ؟

وللإجابة على هذه الأسئلة لابد من طرح الأسئلة التالية :

3ـ هل نظام معلوماتك يحوي على معلومات حكومية حساسة أو صناعية، أو عليمة . . . إلخ.؟

4ـ هل تحوي نظمك على معلومات مالية ذات قيمة لدى المجرمين. . . إلخ؟.

وبناء على الإجابة عن مثل هذه الأسئلة

1ـ فما احتمالية أن يكون نظام المعلومات هدفاً للاعتداء ؟

2ـ ما احتمالية حدوث أي من التهديدات لمعلوماتك ؟

التقديرات الاحتياطية (القبلية) والفورية (البعدية).

هناك نوعان مميزان من تحليل الخطورة.

أ- **التقديرات الاحتياطية (القبلية)** (Proactive assessment) : وهذه الاجراءات تنفذ قبل حدوث المشكلة، وتحديد أهم المخاطر التي تهدد النظام الذي تنوى حمايته. وماهي احتمالات تعرضه للاعتداء، وتحديد الإجراءات المضادة لكل من المهددات واحتمالات التعرض.

ب- **التقديرات الفورية (البعدية)** (Reactive assessment) : ويتم تنفيذ هذه المهمة بعد حدوث المشكلة، وهنا يحدد ما هي الأسباب التي أدت لوقوع الحادثة، وما هي مجالات التعرض التي أدت لذلك، وما هي الإجراءات غير المناسبة التي كانت متوافرة وماهي الإجراءات المطلوب إيجادها الآن. ويشمل تحليل الخطورة الخطوات التالية:

1ـ الضمان (Insurance):

إن سياسات الضمان يمكن أن تحمي ضد الخسارة الناجمة عن التعديات في حرب المعلومات بما في ذلك الأفعال من قبل العاملين داخل المنظمة، وهناك شركات جديدة متخصصة بأمن المعلومات ويمكن أن تعوض عن فقدان المعلومات خاصة من قبل القراصنة، الداخليين، الجواسيس، الفيروسات، السرقة . . . إلح.

2ـ الأداء (Benchmarking):

ويعني عمليات تطوير واستخدام الأعراف الإحصائية لممارسات الأمن المعلوماتية الحرجة، من خلال دراسة المنظمات لتحديد أي ممارسة تستخدم، أو مطبقة فيها. ويمكن إستخدام مقياس احصائية من مثل أن مستوى الأمن في منظمة ما هو 7/ 10، حيث (10) آمنة جداً، و(1) غير آمنة على الإطلاق.

3ـ المسؤولية (Liability):

قد تكون المنظمة مسؤولة عن عدم تشغيل نظمها بطريقة آمنة. وأن العمل الصادق في المنظمة يجب أن يميز عن الاهمال وعدم الاكتراث الذي قد يؤدي إلى خسارة كبيرة للمعلومات، قد يكون بعضها حساساً مثل معلومات الأسلحة، أو صناعات التقنية المتقدمة.

2- **تحديد التهديدات** (Identitfing Threats)

هناك عدد كبير من التهديدات يتراوح بين الجواسيس والمجرمين والمراهقين والغاضبين من قدامى الموظفين إلى الحرائق إلى . . .إلخ. وفيما يلي مجموعة من التهديدات:

1ـ الناس (People) : الناس الغرباء والمستخدمون من أكثر المهددات لأمن المعلومات، الناس هم الذين يكتبون فيروسات الحاسب، ويخرقون نظم الحاسب، ويسرقون البرامج . . . . إلخ. ، الناس مسؤولون عن هذه الأعمال، الموظفون، أكبر مهدد سواء عمداً أو عن طريق الخطأ البشري.

2ـ المعدات (Hardware): تحديد التهديدات التي تواجه معدات المعلومات، هناك ملايين الدولارات قيمة معدات الحاسب التي تسرق سنوياً، أو تلك التي تتعرض لمخاطر أخرى.

3ـ البرمجيات (Software): تعد البرمجيات الإدارة المسؤولة عن تنفيذ المهام في الحاسب، وتتعرض البرمجيات لتهديد ات كثيرة منها النسخ غير القانوني، والسرقة والتعديل والتخريب وتعرضها للفيروسات وحصن طروادة . . إلخ.

4ـ الكوارث الطبيعة والبيئة (Natural & Environemenatl Disasters) تمثل الكوارث الطبيعة الحرائق والفيضانات، والهزات الأرضية خطراً للمباني ولنظم الحاسب، وكذلك الحال بالنسبة للمناخ وأنظمة التبريد وخدمات الكهرباء.

5ـ تحديد رأس المال (Identifying Assets) : لابد من تحديد رأس المال الذي تحاول حمايته في موقعك أو على حاسبك، وهذه تتراوح بين المعدات الفيزيقية إلى المعلومات، والبيانات، وهذه تشمل: البرمجيات (نظم التشغيل، البرمجيات التطبيقية، ملخصات النظم، . . . إلخ.) والمعدات (الحاسب، وحدة المعالجة الرئيسية، ومعدات التخزين، الوسائط المتعددة . . . إلخ.) والبيانات (البيانات الحساسة، والسرية، العمليات والخطط والاحصاء، والمعلومات الشخصية . . . إلخ.) والإدارية (الوثائق، البرمجيات والملفات، العمليات، والإجراءات، والاتصالات، والمصادر البشرية وعمال المبنى . . . إلخ.)، والبيئة الفيزيقية (النظم البيئية، مثل التبريد، والكهرباء، والاضاءة، . . ومعدات النسخ الاحتياطي، والمستودعات . . . إلخ.).

6ـ البيئة (Environment): إن البيئة التي تعمل فيها الأجهزة ذات صلة بنوع تلك البيئة. إن المعلومات عن الموقع الفيزيقي الذي تجمع وتخزن فيه المعلومات بالضرورة أن يصبح نقطة معرضة حيث إن على صاحب تلك المعلومات أن يحرسها. إن مراكز الحاسبات، والشاشات، أو خطوط الاتصالات تمثل

أهداف لأعمال انحرافية وجريمية وتتطلب إجراءات وقاية، ويضاف لهذه العملية بعد آخر عندما يتم تبادل المعلومات من حاسب لآخر.

إن عملية سرقة المعلومات تستغرق أجزاء من الثانية، مما يقلل احتمالية القاء القبض على مرتكيبها، وبالتالي فإن من يقوم بأعمال غير قانونية في هذا المجال يمكن الاستمرار دون أن يكتشف لسنوات، خاصة وأن شبكات المعلومات والاتصالات قد اختزلت المسافة.

3- **تقدير الخطوة** (Risk Assessment)

ويعني تقدير الخطورة العلميات التي تحدد فيما إذا كانت الإجراءات الفعلية الموجودة، أو المتوقع إيجادها مناسبة لحماية مصادر المعلومات من التهديدات المحتملة، إنها تشمل تحديد رأس المال الواجب حمايته، التهديدات المحتملة، واحتمالية وقوعها، والانكشافات التي يمكن أن تستغل، والخسارة المتوقعة من أي اعتداء، والإجراءات الدفاعية (الحماية) التي يمكن تثبيتها، الهدف هنا تحليل الكلفة والفاعلية - Cost) (Effective أي أن الكلفة لحماية المعلومات لا تفوق كلفة المعلومات ذاتها. هناك أعداء محتملون متلصصون، ومتطفلون، منافسون، مجرمون، حكومات أجنبية، إرهابيون . . . إلخ. لكل منهم دافعه الخاص به، ومهاراته التي لها أثر مختلف على كل هدف، هناك أدوات لتقدير الانكشاف(Icove, Seger and VonStorch, 1995).

الدفاع عن المجتمع المعلوماتي

للحكومة دور في الدفاع المعلوماتي على مستوى مسؤولياتها عن الأمن الوطني والاقتصادي، والأمن العام، ونظراً لأن الأمن الوطني جزء من الأمن الكوني (الدولي)، فلابد من مناقشة الدفاع الوطني في السياق الدولي كذلك.

البناء التحتي الوطني المعلوماتي (National Information Infrastructure [NII])

حددت وثيقة البناء التحتي الوطني المعلوماتي الأمريكية خطة عمله بما يلي: معنى واسع يشمل أكثر مساعدات من مادية تستخدم في النقل والتخزين والعمليات وعرض الصوت، والبيانات، والصور، ويشمل : مدى واسعاً ويتسع اتساعاً هائلاً من المعدات بما في ذلك الكاميرات والماسحات ولوحات المفاتيح، والتلفونات،

والفاكسات، والكوابل، والستالايت، والألياف الضوئية، وشبكات الميكروويف، والتلفزيونات، والشاشات، والطابعات . . . إلخ. وسيتعامل البناء التحتي المعلوماتي مع المكونات المادية التقنية، ويتطلب البناء التحتي المعلوماتي بناء أسس للعيش في عصر المعلومات، وجعل هذه التقنيات المتقدمة مفيدة إلى القطاع العام وقطاع الأعمال، والمكتبات، والمؤسسات غير الحكومية. وتعتمد قيمة البناء التحتي المعلوماتي على جودة عناصر أخرى هي :

1ـ المعلومات ذاتها (The Information it self)، وقد تكون على شكل برامج مرئية (فيديو)، أو بيانات علمية أو تخص الأعمال، وصور وتسجيلات صوتية. . . إلخ، ويتوافر منها الآن الكثير.

2ـ التطبيقات والبرمجيات (Applications & Softwares)، والتي توفر للمستخدمين الاتصال بكميات هائلة من المعلومات ومعالجتها وتنظيمها وتلخيصها لتكون رهن اشارتهم.

3ـ مقاييس الشبكات ورموز النقل (Network Standards & Transmission Codes)، وهي التي تسهل الاتصالات والعمليات المتداخلة بين الشبكات وتضمن الخصوصية للأفراد وتضمن الأمن الناقل للمعلومات، بالاضافة إلى الأمن والموثوقية للشبكات.

4ـ الناس (The People)، وغالبيتهم في القطاع الخاص، وهم الذين ينتجون المعلومات ويطورون التطبيقات والخدمات ويبنون التسهيلات ويدربون الآخرين على الاستفادة منها، وغالبية هؤلاء الناس موردون وموظفون ومقدمو خدمات (NIST, ND).

ويتكون البناء التحتي المعلوماتي من ثلاثة أعمدة رئيسة هي : التطبيقات (Applications)، والخدمات (Services)، وطرق البيانات (Bitways)، أو البنية الفيزيقية أو أنابيب البيانات (Data pipes).

ويقصد بالتطبيقات تقنينات المعلومات التي يمكن استخدامها لتحقيق المهمات من خلال مدى من مجالات التطبيقات. أما الخدمات فيقصد بها تقديم بناء قوائم من التطبيقات وتقديم واجهات للعرض، والمحسسات، والمعدات الأخرى (مدخلات / مخرجات). وأخيراً طرق البايتات أو البناء المادي، ويشمل الألياف الضوئية

والمواصلات والأدوات الأخرى الخاصة بالنقل، وبرمجيات التحكم لنقل البيانات من مكان لآخر (NIST, ND).

وفي كندا قدم المجلس الاستشاري الكندي للطرق السريعة للمعلومات في عام (1995م) توصياته الخاصة بـ(15) مجالاً، وكان هناك ثلاثة أهداف وخمس أساسيات، هي:

(أ) الأهداف، وشملت: 1-إنتاج فرص عمل من خلال الابتكار والاستثمار. 2- تقوية السيادة والهوية الثقافية. 3- ضمان الاتصال الشامل بتكلفة معقولة.

(ب) الأساسيات، وهي: 1ـ شبكة شبكات عامة ومتداخلة. 2- تطوير تعاوني بين القطاع العام والخاص. 3ـ المنافسة في التسهيلات والمنتجات والخدمات. 4-حماية الخصوصية وأمن الشبكة. 5ـ التعليم مدى الحياة (روسينبرج، 2000).

وفي الولايات المتحدة الأمريكية كلف المجلس الاستشاري للولايات المتحدة الخاص بالبناء التحتي الوطني المعلوماتي بوضع التصورات الخاصة بهذه البنية في المجالات التقنية، والتجارية، والاجتماعية، والتشريعة، ولقد حدد الأهداف الخمسة التالية:

1-الاستفادة من تقنية المعلومات على مستوى الدولة والمواطن وضمان تطويرها.

2- ضمان الاحساس القومي من خلال التواجد على الشبكة.

3- توسيع الفرص للجميع وضمانها والمشاركة في بناء الطريق السريع للمعلومات.

4ـ تحمل مسؤولية بناء الطريق السريع، من قبل القطاع العام والخاص والأفراد.

5ـ المحافظة على الصدارة العالمية في تطوير الخدمات والمنتجات والسوق المفتوح المنافس.

حماية البنية التحتية الوطنية المعلوماتية

إن زيادة المشاركة في المعلومات داخل البناء التحتي المعلوماتي الواحد وبين القطاعات المختلفة وبين الحكومة يسهل جهود الأفراد والمالكين للمعلومات من تحديد الثغرات واكتساب الأدوات اللازمة لحماية المعلومات. وتتطلب حماية البنية التحتية

المعلوماتية تكامل جهود الوكالات والأجهزة الحكومية والخاصة. وهذا يتطلب تبني سياسات تتأقلم مع الثقافة المتغيرة، والتطورات التقنية المتسارعة. وللحكومة دور هام في حماية البنية التحتية المعلوماتية بالتعاون مع قطاع الصناعة والإدارات الحكومية المحلية. كما أن للبحث العلمي أهمية خاصة في تطوير الوسائل المناسبة في حماية البنية التحتية المعلوماتية.

قامت الولايات المتحدة أولاً بإنشاء مركز التنسيق لفريق الحاسب لاتصالات الطوارئ والمعروف بـ (CERT/CC) في جامعة كارنجي ـ ميللون (Carnegie - Mellon) عام 1988م بعد حادثة كبيرة أصابت الأنترنت وعطلت الآلاف من الحاسبات، حيث أوجد الـ (CERT/CC) قسم وكالة مشاريع البحث للدفاع المتقدم (وهي التي أوجدت الإنترنت) وتعمل على المراقبة وحل المشكلات التي تعترض الشبكة.

والمؤسسة الثانية تم إيجادها ضمن الحكومة الفدرالية الأمريكية بما في ذلك القسم المعروف باسم (Department of Energys Computer Incident Advisory Capability (CIAC) . ووكالة حماية نظم المعلومات (ASSIST)، وفي عام (1989م) مركز الأمن والاستجابة للحوادث (Incident Response Security Teams (FIRST) للتنسيق بين هذه المراكز، وهذا أدى إلى تكوين مركز فدرالي عرف باسم المركز الفدرالي للاستجابة لحوادث الحاسب (Fed CIRC). وثانياً تكوين اللجنة الرئاسية لحماية البناء التحتي الحساس (Perident Commission on Critical Infastructue Protection (PCCIP) عام (1996م).

1ـ المبادئ العامة لأمن النظم والمعروفة باسم (GSSP) أو (GASSP)

في عام (1990م)، أنشئت لجنة سياسة الاتصالات والحاسب والمعلومات (Information, Computer, and Communication Policy [ICCP]) التابعة لمنظمة التنمية والتعاون الاقتصادي (Organization For Economic Cooperation and Development [OECD]) مجموعة من الخبراء لإعداد إرشادات لأمن نظم المعلومات، ولقد شملت المجموعة وفوداً من دول منظمة الدول الصناعية الكبري (OECP)، ومن خبراء في القانون والرياضيات، وعلم الحاسب، والقطاع الخاص،

ولقد قدمت المجموعة إلى إرشادات لأمن نظم المعلومات (Guidelines for the Security of Information Systems) لإقرارها من (ICCP)، ولقد قبلت هذه الإرشادات من قبل (ICCP) في عام (1992م)، واعتمدت من (24) من الدول الأعضاء في منظمة الدول الصناعية الكبرى (OECD)، ولقد كتبت الإرشادات لتناسب جميع نظم المعلومات في القطاعين العام والخاص، ولقد تم تحديد تسعة مبادئ هي :

1ـ المحاسبة (المسؤولية) (Accountability): يجب أن يكون هناك مسؤولية ومحاسبة للمالكين، والمقدمين للخدمة، ومستخدمي نظم المعلومات والأطراف الأخرى المعنية بأمن نظم المعلومات واضحة ومحددة.

2ـ الوعي (Awareness): لتفعيل الثقة في نظم المعلومات فإنه يتوجب على المالكين والمقدمين للخدمة، ومستخدمي نظم المعلومات، والأطراف المعنية أن يكونوا جاهزين في إدامة الأمن للحصول على المعرفة المناسبة وليعلموا ما يتعلق وجود مقدار توافر الإجراءات العامة، والممارسات، والاحترازات لأمن نظم المعلومات.

3- الأخلاقيات (Ethics): أن تزود نظم المعلومات ونظم أمن المعلومات وتستخدم بطريقة تخدم حقوق وشرعية اهتمامات الآخرين.

4ـ تعددية الحقول (Multidesciplinary): يجب أن تأخذ الإجراءات والممارسات، والاحترازات لأمن نظم المعلومات بالحسبان، وتتضمن جميع الاعتبارات ذات الصلة ووجهات النظر بما في ذلك وجهات النظر الفنية، والإدارية، والتنظيمية، والتشغيلية، والتجارية، والتربوية، والقانونية.

5ـ التناسب (Proportionality): يجب أن تتناسب مستويات الأمن، والاحترازات، والممارسات، والإجراءات، وتكون مناسبة لقيمة نظم المعلومات، ومقدار الاعتماد عليها، وإلى شدة واحتمالية ومقدار الأذى المحتمل، وتتباين متطلبات الأمن بالاعتماد على نظم أمن المعلومات.

6ـ التكامل (Integration): يجب أن تتناسق وتتكامل الإجراءات، والممارسات، والاحترازات الخاصة بنظم المعلومات بين كل منها، ومع كل من الإجراءات والممارسات والاحترازات للمنظمة لتكوين نظام أمني متناغم.

7ـ قنوات الوقت (Time lines): يجب على كافة الأطراف الحكومية والخاصة على المستويين الوطني والدولي التعرف بطريقة متناعمة زمنياً لمنع الاستجابة للخروق في نظم أمن المعلومات.

8ـ إعادة التقييم (Reassessment): يجب أن يعاد تقييم نظم المعلومات دورياً كنظم معلومات والمتطلبات لأمن متباينة عبر الوقت.

9ـ الديمقراطية (Democracy): يجب أن تكون نظم المعلومات متوافقة مع الاستخدام الشرعي وتدفق البيانات والمعلومات بمجتمع ديمقراطي (Denning, 1999, pp 397-398).

وتتناول هذه الإرشادات مجالات عديدة من التطبيقات بما في ذلك تطوير السياسات، والتربية، والتدريب، وانفاذ القانون... إلخ.، والتعاون بين القطاع الخاص، والقطاع الحكومي بهدف تطبيق احترازات وإجراءات وممارسات يتناغم لنظم أمن المعلومات.

2ـ الهيئة الرئاسية لحماية البناء التحتي الحساس

في 15/ 7/ 1996 أمر الرئيس الأمريكي السابق بل كيلنتون بتشكيل فريق عمل لحماية البناء التحتي الحساس (President\s Commission on Critical Infastructure Protection [PCCIP])، وذلك لدراسة الأبنية التحية الحساسة والتي تشكل أنظمة دعم الحياة للمجتمع، وتحديد مدى تعرضها للتهديدات، وتنفيذ استراتيجية لحمايتها في المستقبل. ولقد تم تحديد ثمانية أبنية معلومات تحتية حساسة هي:

1ـ الإتصالات.

2ـ البنوك والمال.

3ـ الطاقة الكهربائية.

4ـ توزيع الوقود والغاز.

5ـ التخزين.

6ـ مصادر المياة.

7ـ المواصلات.

8ـ خدمات الطوارئ والخدمات الحكومية (PCCIP, 1997).

وتتنوع تهديدات البناء التحتي الحساس فمنها تهديدات فيزيقية وفضائية (Cyber) وأخرى تتعلق بالحوادث والكوارث الطبيعية، والأخطاء، والداخليون، وقراصنة الترفيه، والنشاطات الإجرامية، والتجسس الصناعي، والاستخبارات الأجنبية، والإرهاب، وحرب المعلومات. وهناك زيادة في الاعتماد على هذا النوع من البنى التحتية، وهناك زيادة في تعرضها، وعدم وجود وعي عن هذا التعرض لدى استخدم.

لقد نادت اللجنة باستراتيجية عملية (Action) لحماية البناء التحتي من خلال التعاون الصناعي وتبادل المعلومات، وبرامج التوعية العامة، والتعليم، وإعادة النظر بالقانونين المتصلة بحماية البناء التحتي، وتطوير برامج البحث والتطوير. ولقد حددت اللجنة خمسة مجالات للشراكة بين الحكومة ومالكي البناء التحتي ومشغليه ضرورته :

1ـ تكوين السياسات (Policy Formation). يمكن للحكومة أن تقدر التهديدات الناجمة ويمكن للمالكين والمشغلين من تقدير الثغرات الأمنية، ومعاً يمكنهم أن يقدر وا الخطورة على المستوى الوطني، والأهداف، والاستراتيجيات، والسياسات.

2ـ الوقاية والتخفيف (Prevention & Mitigation). على المالكين والمشغلين أن يتفحصوا الثغرات في نظمهم وفي الشبكات ويمكن وضع إجراءات حماية وعملية لتحقيق مستويات الضمان المستهدفة، ويمكن للحكومة أن تدعم جهود البحث والتطوير والوعي والتعليم وتقدير التهديدات وتشجيع القطاع الخاص على تطبيق أفضل الممارسات.

3ـ تبادل المعلومات وتحليلها(Information Sharing & Analysis). وهنا يقدم كل طرف ما لديه من معلومات وتيم تحليل هذه المعلومات وتحديد الثغرات ووضع الاجراءات اللازمة لسدها.

4ـ ردة الفعل (إدارة الحوادث)(Counteraction Cincident Management and Reconstitution) (Consequences Management). في هذا السياق يحدد ما يحدث بشكل غريب في البناء التحتي.

5ـ الاستجابة وإعادة البناء إعادة المؤسسة (إدارة النتائج) (Response, Restoration). إن مسؤولية الاستجابة للحاجات الأساسية الناجمة عن

الكوارث تقع على عاتق الدولة، أما إعادة النباء وإعادة التأسيس فمسؤولية المالكين والمشتغلين، ويتطلب إعادة البناء، وإعادة المؤسسة تضافر جهود القطاعين العام والخاص.

ولقد اقترحت اللجنة بناء وطنياً لضمان البناء التحتي مكون من سبعة عناصر هي:

1ـ مكتب وطني لضمان البناء التحتي ويمكن أن يتبع هذا المكتب إلى المجلس الوطني للأمن، ومكتب الرئيس، ويدار من أحد مساعدي الرئيس تشمل الواجبات والوظائف صياغة السياسة، وإغفال نشاطات الحكومة في تأمين البنية التحتية، ومواضيع الأمن الفضائي، والتنسيق في الدعم الفضائي لعمليات اتخاذ القرار الموجودة والمخططة في انفاذ القانون والأمن الوطني، ومواجهة الإرهاب، ومجالات الاستخبارات. كما يمكن أن يسهل المكتب الوطني، تكوين تأمين للبناء التحتي ليشمل تقدير الخطر الوطني، ودمج منظور القطاع العام، والقطاع الخاص، وتحديد أهداف وطنية لتطوير استراتيجيات تطبيق، وتقديم تشريعات، وتفعيل أخرى، وتقدير الحاجة للتنظيمات الجديدة.

2ـ مجلس ضمان البنية التحتية، وهذا يمكن تعيينه من الرئيس ويتكون من مدراء المكاتب من مجالات البناء التحتي الحساس، وكبار موظفي الدولة، وممثلي الولايات والحكومات المحلية، ويمكن أن يلتقي دورياً لمناقشة سياسات ضمان البنية التحتية وصياغة التوصيات المناسبة للرئيس ويمكن لهم أن يراجعوا مشاريع من قطاع الصناعة وأن يقدموا قيادة، ونصحاً، ودعماً للتعلم وجهود التوعية.

3ـ مكتب دعم الضمان للبناء التحيتي: يمكن لهذا المكتب أن يقدم دعماً وظيفياً وإدارة للمنظمات الفيدرالية المشاركة في تأمين البناء التحتي، وتقديم مساعدة مباشرة في مشاركة القطاع العام والخاص، وتوجه نشاطاته من خلال المكتب الوطني، ويمكن أن يقع هذا المكتب في قسم التجارة، ويدعم تكوين السياسة والوقاية والتخفيف من التهديدات، ومساعدة المكتب الوطني في إدارة المشاركة بالمعلومات ومركز التحليل.

4ـ منسقو القطاعات لتسهيل مشاركة المعلومات بين المقدمين والحكومة، وحيث تقود القطاع في تحديد الطريقة المثلى في المشاركة بالمعلومات اللازمة لحماية البناء التحتي من قبل الحكومة والمالكين والمشغلين الذين يمثلونهم، وقد يمثلون بوابة داخل القطاع لتقدير نشاطات المخاطرة.

5ـ مشاركة المعلومات ومراكز التحليل، ويتكون المركز من ممثلين عن الحكومة، والصناعة ويعملون معاً لتلقي المعلومات من جميع المصادر، ويحللونها لرسم خلاصات حول ما يجري في البناء التحتي، وإعلام المستخدمين في الحكومة، والقطاع الخاص، ويركزون على جمع معلومات استراتيجية تتعلق بمهددات البناء التحتي، والتعرض (الانكشافات)، والممارسات، والمصادر التي تمكن من تحليل فعال لفهم أفضل للبعد الفضائي للبناء التحتي. وقد تتلقى تقارير لحوادث غير عادية، وتجهيز الخبراء والمتشارين. وقد يكون هذا المركز في القطاع الخاص من مثل (CERT/CC) في كارنج ميلون (Carnegie Mellon) أو في أي (CERT) أو أي مركز بحوث.

6ـ المركز الوطني لإعلان الطوارئ (التحذير) الفوري والتنبؤ الفوري في أي هجوم فيزيقي أو فضائي على البناء التحتي، وتتبع مسؤولية المركز بـ(FBI) حيث بدأت في بناء وحدة متعددة الأطراف للمراقبة وتحليل التهديد، حيث يمكن أن تصمم أي إشارة لتهديد.

ولقد واجهت الهيئة الرئاسية (PCCIP) بعض المشكلات القانونية في التطبيق، حيث إن القطاع الخاص بحاجة إلى تأكيد وضمان بأن المعلومات الحساسة المشتركة مع الحكومة محمية وغير متاحة للأطراف الأخرى المنافسة. كما ترى الهيئة أن تعمم الأحكام الجنائية المطبقة ـ في مجال التعديات في الحاسب والاحتيال الحاسوبي وسوء استخدام الحاسب والسرقة للعلامات التجارية والأسرار التجارية ـ إلى الأشكال الأخرى الجرائم الإلكترونية والجرائم المتصلة بالتكنولوجيا وتكنولوجيا المعلومات. كما أوصت الهيئة الرئاسية (PCCIP) بتوسيع البرامج البحثية والتطوير الهادف إلى تطوير الإمكانيات الضعيفة حالياً من مثل كشف التطفل.

القرار الرئاسي (التوصيات) في 22/ 5/ 1998م أعلن البيت الأبيض أن القرار الرئاسي التوجيهي (President Decision Directive)، والذي شمل مراجعة إلى توصيات (PDD63) الهيئة الرئاسية (PCCIP) وبنى عليها التوصيات التالية:

1ـ تحديد هدف موثوق متداخل وبناء تحتي لنظام معلومات أمن مع حلول العام (2003م)، وزيادة الأمن للنظم الحكومية في عام (2000م) من خلال تكوين فوري لمركز وطني للتحذير / للهجوم والاستجابة له من خلال بناء الإمكانيات التي تحمي البناء التحتي الحساس من الأفعال المتعمدة بحلول العام (2003م).

2ـ مناقشة انكشاف البناء التحتي الفيزيقي والفضائي للحكومة الفدرالية من خلال الطلب من كل قسم ووكالة العمل لخفض تعرضها لتهديدات جديدة.

3ـ الطلب من الحكومة الفدرالية أن تعمل كنموذج لبقية الحكومات في كيفية تحقيق حماية البناء التحتي.

4ـ بحث المشاركة التطوعية للصناعة الخاصة لتحقيق الأهداف العامة في حماية البناء التحتي الحساس من خلال الشراكة بين القطاعين العام والخاص.

5ـ حماية حقوق الخصوصية والدعوة للاستفادة من قوى السوق بهدف تقوية القوة الاقتصادية الوطنية وحمايتها.

6ـ البحث عن المشاركة الكاملة والمدخلات من الكونجرس.

ولقد حدد القرار الرئاسي (PDD63) البناء اللازم لتحقيق هذه الأهداف :

1ـ المنسق الوطني والذي تشمل مهامة الابنية التحتية الحساسة والإرهاب الأجنبي، والتهديدات للتدمير الشامل المحلي وعين لها مستشار الأمن الوطني.

2ـ المركز الوطني لحماية البناء التحيتي (NIPC)، والموجود لدى الـ(FBI)، ويشمل ممثلين عن (FBI)، ووزارة الدفاع، ووكالة المخابرات، والطاقة، والمواصلات، والمخابرات، والقطاع الخاص، ويقدم المركز الوسائل المسهلة، والتنسيق لاستجابة الحكومة الفدرالية للحوادث، والتعديات، والتحقيق في التهديدات، ومراقبة جهود إعادة المؤسسة.

3ـ مركز التحليل وتبادل المعلومات (ISAC)، ويبنى من القطاع الخاص بالتعاون مع الحكومة الفدرالية، ولقد شجع القرار (PDD63) تكوين (ISAC)، ولكن يرجع للقطاع الخاص لعمله، يخدم المركز كوسيط في جميع المعلومات وتحليلها وتنظيفها، ونشر معلومات القطاع الخاص إلى كل من الصناعة و (NIPC).

4ـ المجلس الوطني لضمان البنية التحتية (NICS)، ويتكون من القادة في القطاع الخاص، وكبار الموظفين المحليين، ويعمل المجلس على تقديم إرشادات لتكوين سياسة لخطة وطنية.

5ـ مكتب ضمان البنية التحتية الحساسة (CIAO) داخل قسم التجارة، ويقدم المكتب الدعم إلى التنسيق الوطني مع الوكالات الحكومية.

تهدف(NIPC) إلى العمل في الوقاية، والمنع، والاستجابة. . . والتحقيق في التعديات على البناء التحتي الحساس، أن تدير تحقيقات الـ(FBI) التي تتضمن جرائم الحاسب والتهديدات الموجه إلى البناء التحتي الوطني.

وينسق مكتب ضمان البنية التحتية الحساسة (CIAO) تطوير الخطة الوطنية المبنية على خطط القطاعات، وتشمل الخطة الوطنية بحد أدنى على :

1ـ تقدير الانكشاف الأولى متبوعاً بتقدير دوري لكل قطاع من الاقتصاد، وكل قطاع حكومي، ربما يكون هدفاً لهجوم.

2ـ خطة إصلاحية (تعويضية) للتخفيف من الاستغلال القصدي للانكشافات المحددة.

3ـ مركز وطني للتحذير من الهجمات المهمة على البنية التحتية.

4ـ خطة للإستجابة للهجمات الراهنة من أجل فصل الضرر وتقليله وكذا التأثير للإعادة الفورية للخدمات الأساسية.

5ـ برامج تربوية وتوعوية لتحسيس الأفراد بأهمية الأمن.

6ـ البحث الفدرالي والتطوير اللذان يساعدان في تطوير نشر التكنولوجيا لتقليل الانكشافات.

سياسات التشفير

تعد سياسة التشفير (Encryption) من أكثر التحديات الجدلية التي تواجه مجتمعات اليوم. وتظهر الصعوبة بسبب ظهور وظيفتين متعارضتين هما: صنع الترميز (التشفير) (Code Making)، وفك الترميز (Code Breaking).

أ ـ صنع الترميز (Code Making)

يعني مصطلح صنع الترميز أو التشفير تطوير منتجات تشفير تستخدم لحماية الخصوصية والموثوقية (ليس للتعريف) وهنا ثلاثة أهداف رئيسة:

1ـ حماية الإتصالات وحفظ المعلومات من المنافسين والأعداء، ومنظمات الأعمال تحتاج إلى التشفير لحماية ملكية المعلومات من التجسس المؤسسي والاقتصادي وحماية الثروة. والأفراد بحاجة إلى الحماية من المتطفلين (Snoops)، والأعداء، واللصوص، والحكومات القمعية. وتحتاج الحكومات التشفير لحماية الأسرار العسكرية والدبلوماسية ولحماية الاتصالات المتعصلة بالتحقيقات الجنائية والإرهابية من أولئك الذين يحقق معهم، ولحماية المعلومات الأخرى الحساسة، تلعب صناعة التشفير دور مهم في الوقاية من الجريمة. ويحتاج المستخدم العادي إلى التشفير الآمن والسهل والمتضمن في البرمجيات التي يستخدمها وفي الشبكات. أنه بحاجة إلى منتج موثوق، وهناك حاجة إلى التشفير الذي يحمي الاتصالات الوطنية والدولية من الحكومات الأجنبية والمنافسين وأن يكون ذو كلفة مادية معقولة. يرغب المستخدمون بدفع كلفة شراء برامج تشفير تفوق كلفة المادة المحمية أصلاً.

2ـ بيع منتجات التشفير وخدماتها يهتم المنتجون في إنتاج سلع وبرمجيات ومواد بأقل كلفة ممكنة. وهم مهتمون بالأسواق العالمية وليس السوق المحلية فقط.

3ـ إن شراء المكونات الفكرية من صنع التشفير يساهم في تقدم هذا الحقل، فالأكاديميون والباحثون والهاون يرغبون بدراسة التشفير دون قيود على ما يفعلون أنهم يأملون بالمساهمة تقدم المعرفة في مجال التشفير والاستفادة مما هو متاح على الإنترنت وخاصة للباحثين والمهتمين.

ب ـ فك التشفير (Code Breaking)

يعني مصطلح فك التشفير الحصول على الوصول النصي الخاص بالبيانات المشفرة بطريقة ما غير عملية إزالة التشفير الطبيعة (Decryption) والمستخدمة من المستقبل المعني بالبيانات. ويمكن حل التشفير، أو إزالته من خلال الحصول على مفتاح التشفير بواسطة مفتاح خاص لخدمات الاستعادة أو من خلال إيجاد مفتاح بواسطة تحليل التشفير، هنا خمسة أهداف:

1ـ التأكيد على أن المعلومات التي يمكن الوصول إليها كما هو في حالة (مفاتيح حل التشفير) مفقودة. ومدمرة أو مخربة، ومن المنظور المؤسسي، فإن فقد مفتاح حل التشفير تفقد المعلومات قيمتها. وبالتالي لابد للأفراد أو المؤسسات من فك (كسر) التشفير لحفظ المعلومات.

2ـ التجسس على أحد المعارضين، الأجهزة الأمنية ترغب في حل التشفير عن الاتصالات واعتراضها كجزء من العمليات الاستخبارية الأجنبية لحماية المصالح الوطنية ودعم العمليات العسكرية. ومؤسسات إنفاذ القوانين، تسعى إلى فك التشفير للحصول على المعلومات المتعلقة بالإرهاب ومكافحة المخدرات، والتحقيق والتعقيب ومتابعة المجرمين.

3ـ بيع المنتجات المقرصنة والخدمات لأصحاب البيانات والحكومات الصناعة في حالة منافسة في صناعة التشفير وفي فكه.

4ـ يتضمن بيع مكونات فكرية لفك التشفير المشاركة في عرض مشاريع على مستوى عام.

ج ـ فحص التشفير وقوته:

يشمل المهتمون بفعل الترميز مثله مثل صنع التشفير، المؤسسات والحكومات، والوكالات، والمطورين، والأكاديميين، والهواة . . . إلخ. أهدافهم على المستوى الوطني والأمن الوطني، والأمن العام، والوقاية من الجريمة، والتحقيق، والخصوصية، والحرية الأكاديمية، وأحياناً بعد فك التشفير ضد الخصوصية.

السياسات الدولية في التشفير:

لقد قدمت منظمة التطوير والتعاون الاقتصادي (OECD) عام (1996م)، إرشادات (خطوطاً عامة) لسياسة التشفير آخذة بالحسبان المستوى الوطني والدولي اللازم للتعاون في هذا المجال. وتفرع عن هذه الإرشادات المبادئ الثمانية التالية :

1ـ الثقة في طرق التشفير.

2ـ الاختيار من طرق التشفير.

3ـ التطوير السوقي لطرق التشفير.

4ـ المعايير لطرق التشفير.

5ـ حماية خصوصية البيانات.

6ـ الوصول القانوني.

7ـ الحماية القانونية.

8-التعاون الدولي (يخص كل دولة).

وفي بعض الدول كالولايات المتحدة فإن تصدير تكنولوجيا التشفير مضبوط من خلال تنظيمات مستنتجة من قانونين هما :

قانون ضبط التصدير العسكري (Arms Export Control Act [AECA]) لعام (1949). وقانون إدارة التصدير (Export Administration Act [EAA]) والذي يغطي المواد ذات الاستخدام المزدوج (مدني ـ عسكري).

التهديدات الخارجية:

مع زيادة الترابط الكوني ومع زيادة التجارة الإلكترونية زادت التهديدات من المستخدمين الموثوفين مثل المزودين القانونيين والمستشارين والعملاء، وجاءت أكثر التهديدات الخارجية من الدخلاء (Chackers) (25%)، والمستخدمين غير المصرح لهم، وإرهابين الحاسب.

في الدراسة المسحية الموسوم «المسحية السنوية الثانية لأمن المعلومات (GIS) عام (1998م)، والتي شملت (4300) شخص تقني في (35) دولة والذين أكدوا ظهور موضوع الربط وموضوع التجارة الإلكترونية (AABS, 1998). ففي (66%) من العينة يستخدمون النوافذ في مجال العمل وخدمات الإنترنت متوافرة في (46%) من منظماتهم، و(42%) يتوافر لديهم نظم رئيسة (شبكات) ويستخدم نظام (Unix) في (40%) من منظماتهم، و(80%) لديهم وصول عن بعد مع منظمتهم وهناك (6%) من المنظمات توفر (20%) من الوصول عن بعد لموظفيهم، والهاتف (Dial up) هو أكثر الوسائل في الوصول حيث استخدمه حوالي (69%)، والخطوط المستأجرة (29%)، والانترنت (20%)، والشبكات الخاصة التخيلية (VPNs) (70%). ويستخدم (65%) من العينة أكثر من تقنية في عملهم.

وفي مجال أمن المعلومات تبين زيادة الوعي في المخاطر التي تواجه المنظمات على خلال (6) سنوات مضت والتي نفذت فيها الدراسة كمسح سنوي. وتبين أن حوالي (75%) من أفراد العينة لديهم ثقة بإمكانية الدفاع الذاتي ضد أي عدوان مقارنة بـ(41%) عام 1997م. ومن بين الـ(75%) الواثقون. ومن بين المناطق التي شملتها الدراسة أن آسيا / الباسفيكي كانوا الأقل ثقة (25%) في أساليب الحماية الداخلية والشرق الأوسط / شمال أفريقيا (24%) أمريكيا الشمالية.

ولا بد من إجراء بعض التحريات الأولية عن الموظفين قبل تعيينهم وتحديث المعلومات عنهم أولا بأول، والإطلاع على الاتفاقيات الموقعة على الموردين وأصحاب العقود وفيما إذا كانت المسؤولية محددة. ومن المفيد تعميم السياسة الأمنية في المؤسسة، وتدريب الموظفين، وتدريب المشرفين لتحديد والاستجابة لمشكلات الموظفين الحاليين أو السابقين، وعدم ضمان الميزات تلقائياً، وتحديد ميزات الدخول وفق المكانة المهنية في المنظمة، وعند ترك الموظفين للعمل حتى لو كان ذلك طواعية فيجب أن تراجع التزاماتهم، وإلغاء أية امتيازات قد منحت لهم بحكم موقعهم، واستعادة مفاتيح أو بطاقات دخول، ومراجعة ملفاتهم بدقة.

وهناك عدد من البرامج الجاهزة تتيح للشركات القيام بهذه الرقابة منها برنامج سيرف ووتش (Surf Watch) النسخة المهنية، وبرنامج ويب سنس (Web Sense)، وبرنامج لتيل برذر (Little Brother). كما وهناك برامج تتيح للوالدين مراقبة أبنائهم على الشبكة كبديل لبرامج الترشيح، مثال ذلك برودنس (Prudence). ويمكن أتمتة عمليات المراقبة هذه لمعظم هذه البرامج ولديها امكانيات هائلة في المراقبة.

ولاكتشاف المتطفلين ومجرمي الإنترنت يستطيع إداريو النظام والشبكة معاينة، ومراقبة ملفات المراجعة، ومعلومات حالة النظام، والحركة على الشبكة، إضافة لاستخدام البرامج الجاهزة.

بعض هذه البرامج يعمل فورياً، ويقوم باكتشاف الدخول، والتلصص حال وقوعه، ولها إمكانيات إيقاف المتلصص عند حده قبل أن يستفحل الضرر وتجميع البيانات لمقاضاته مستقبلاً، وتتوقع مجموعة ابردين (Aberdeen Group) الاستشارية أن ينتعش سوق هذه البرامج انتعاشاً كبيراً مثل سوق جدر الحماية الأمنية.

الفصل الخامس عشر

مخابئ المعلومات

مقدمة

إحدى الطرق لحماية مصادر المعلومات الحساسة، والهامة هي عن طريق إبقائها بعيدة عن الأنظار، أو بعيدة عن مكائد المعتدين، أو خلف قفل مادي أو رقمي. يتناول هذا الفصل بالشرح سبع وسائل وطرق من الحماية وهي:

1ـ الحماية الفيزيقية (Physical Security).

2ـ التشفير (التعمية)(Encryption).

3ـ المخابئ (Steganography).

4ـ المجهول (الغفلية) (Anonymity).

5ـ الترشيح (Sanitization).

6ـ التخلص من نفايات المعلومات (Trash Disposal).

7ـ درع المعلومات (Shielding).

إن الهدف من هذه الوسائل والطرق هو حماية خصوصية وموثوقية المعلومات وتكاملها بعيدة عن الخصوم، وتمثل هذه الوسائل والطرق الوقاية القبلية للمعلومات من التعديات، والإنذار المبكر عند حصول تعديات عليها.

1ـ الحماية الفيزيقية (Physical Security):

الأمن الفيزيقي يحمي موقع معدات المعلومات (المبنى، غرفة الحاسب، الحاسب نفسه، المعدات المرافقة) (الأقراص، الأشرطة... إلخ.) غرفة المعدات، غرفة الاتصالات ومعداتها.

إن الأمن الفيزيقي عملية حيوية للدفاع عن أي جريمة معلومات، وبالتالي فهي تشمل الإجراءات التي يجعل من الوصول للمعلومات عملية صعبة، وعلى الرغم من إجراءات الأمن الأخرى يبقى الأمن الفيزيقي أساساً.

إن إجراءات الأمن الفيزيقي للمعلومات تمنع حدوث كوارث أو على الأقل تقلل من آثارها، والتي تتراوح بين الإجراءات البسيطة إلى المعقدة، مثل أنظمة قطع التيار،

وضبط الدخول للمبنى . . إلخ. فإذا كان الخرق للنظام وللحاسب عن بعد (Remote) من قبل قراصنة أو عابثين فلا بد من البحث في الأمن الفيزيقي وضبط الدخول للنظام، فقد يكون أحدهما أو كليهما. ولابد من تحديد المكان الذي تم فيه خرق الأمن الفيزيقي. وتتركز أساسيات الأمن الفيزيقي في (1) وضع العوائق التي تحول دون وصول الدخلاء والعابثين والمخربين والمجرمين إلى المعلومات. (2) ضبط الدخول وعدم السماح إلا لمن لهم الحق القانوني في الدخول والوصول للمعلومات. (3) المراقبة لمعرفة حركة الدخول غير القانوني، والتعامل مع أية حالة دخول غير شرعي.

وسائل الحماية الفيزيقية :

أ. **العوائق** (Barriers)، ويتعلق ذلك بالدفاع القوي عن المعلومات مثل الحراسة والعوائق المعدنية أو البنائية، أو الإلكترونية أو الكهربائية. وتمنع هذه العوائق الدخلاء من معرفة ما بداخل المبنى، وتشمل إغلاق أبواب المبنى لإبعاد الغرباء والمتطفلين والمجرمين عن الدخول إلى منطقة المعلومات، وتحصين موقع معدات المعلومات (كالحاسبات) بشكل مناسب.

1ـ **المفاتيح والأقفال** (Physical Locks & Keys).

تستخدم المفاتيح والأقفال لحماية أي وسط مادي، ويشمل ذلك البيئة المادية والأوراق والأقراص، وشرائط الكمبيوتر، ونظم الكمبيوتر، والاتصالات. وتوضع على أبواب المباني، والمكاتب، والبوابات الخارجية، والخزائن، والطاولات، وخزائن الملفات . . . إلخ، ويعمل القفل كجهاز تحكم سلبي لمنع الولوج وكآلية لإخفاء محتويات الشيء المقفول، والتقنيات في هذا الصدد تشمل الأقفال المادية، والأقفال المركبة (Combination Locks)، ولوحة المفاتيح الإلكترونية.

وتعد المفاتيح والأقفال أول خط دفاع ضد العابثين والمتطفلين بالمبنى، وهذا ليس بالأمر السهل، حيث إن كل موظف في مجتمع اليوم لديه جهاز حاسب يعمل عليه. وفي مثل هذه البيئة فإن هناك صعوبة في إغلاق كل جهاز ووضع قفل له. ويفضل أن تكون الأجهزة الأكثر حساسية مرتبطة بشكل مركزي.

2 ـ **الحماية من الكوارث الطبيعية** (Natural Disasters) :

تتعرض مواقع المعلومات (الحاسبات والمعدات الأخرى) لتهديد الكوارث الطبيعية، والحرائق، والهزات الأرضية، والزلازل . . . إلخ.) وجميعها تهدد الأمن الفيزيقي للمعلومات، والخسارة في المعلومات لا تتوقف على خسارة المعدات والأجهزة، وإنما إلى فقدان المعلومات والبيانات والبرمجيات. ويمكن حماية المعلومات من أخطار الكوارث الطبيعية من خلال عدة وسائل منها جدران الحجر، ووضع عوائق تحول دون الوصول إلى أمكنة المعلومات (الحاسب) ووضع منبهات للحريق، ووضع نظم غلق تلقائية لنظم الحاسب والتبريد عند حدوث حريق، ووضع طفايات الحريق قريبة من غرف الحاسب وتطبيق السياسات المضادة للتدخين، ووضع الحاسبات في أمكنة مضادة للحريق. كما يفضل أبعاد الحاسبات عن الطوابق الأرضية (المخازن)، ووضع مجسات للمياه.

3 ـ **الحماية من التهديدات البيئية** (Environmental Threats) :

تعد التهديدات البيئية مثل الكهرباء والحرارة، وأنظمة التبريد جزءاً من الأمن الفيزيقي للمعلومات، والكهرباء مهدد كبير لنظم الحاسب الذي يمكن أن يهدد أمن الكتب من المعلومات. أما معدات الحاسب فهي حساسة لأي تغير في شدة التيار الكهربائي أو نوعيته. ويمكن أن تفقد المعلومات جراء أي خلل كهربائي قد يؤثر على الحاسب. ويمكن حماية المعلومات في مثل هذه الحالات من خلال غلق الحاسبات عند حدوث برق أو صواعق، والمحافظة على حرارة (10ـ26) درجة مئوية في غرف الحاسب، والرطوبة (35-50%)، ووضع جهاز تبريد خاص بغرف الحاسب، كما يفضل استخدام المرشحات لنظام التبريد والتدفئة، كما يفضل وضع منظم كهرباء في حالة عدم استقرار التيار الكهربائي.

ب ـ **ضبط الدخول** (Access Control)، وتشمل الأدوات المستخدمة التي تحول دون دخول الغرباء والدخلاء ووصولهم إلى المعلومات، ومن أهم وسائل ضبط الدخول أدوات قراءة بصمة اليد، وكلمات السر، والصور الشخصية، والحراسة الشخصية، وأن الحصول على إذن دخول للمبنى أو لموقع المعلومات لابد من يمر العابر بنوع من اختبار الهوية من مثل الصوت، أو الرقم . . . إلخ.، وذلك لإثبات أن الشخص العابر (الداخل) للمبنى هو ذات الشخص المسموح له بالدخول.

وتشمل مثل هذه الإجراءات:

(1) شيء تعرفه (كلمة المرور)

(2) شيء تملكه (مفتاح، بطاقة دخول... إلخ).

(3) شيء منك (بصمة يد).

كما يمكن استخدام وسائل أخرى في ضبط الدخول منها التشفير لمنع الدخلاء وحماية الكوابل التي توصل التيار الكهربائي والحاسبات ببعضها البعض. جميع هذه الإجراءات يمكن أن تستخدم للأمن الفيزيقي، ويقاس الأمن الفيزيقي بوقت الدخول (Penetration time) وهو كم من الوقت يحتاج المتطفل (المقتحم) (Intruder) لدخول الدفاعات الفيزيقية والهدف هنا تأخير دخول المتطفل أكثر وقت ممكن ليتمكن رجل الأمن والشرطة من الوصول للمكان.

ج. **المراقبة** (Surveillance). وتشمل وضع الأدوات الكاشفة مثل (كاميرات المراقبة) لأي محاولة دخول غير قانونية، ففي الوقت الذي يتم فيه كشف مثل هذه المحاولات يواجه الدخلاء بالحرس، ويلجأ الدخلاء إلى التخفي في ملابس عمال النظافة أو الصيانة، على العاملين ومسؤولي الأمن التنبه لذلك.

1ـ **التفتيش المنتظم** (Regular Inspections)

يفيد التفتيش المنتظم في التأكد من أن جميع نقاط الثغرات الممكنة قد تمت معاينتها. ويفضل أن يكون التفتيش من أفراد لا يعملون في المكان ذاته (القسم أو الطابق). ويمكن استخدام المعلومات التي يتم الحصول عليها من خلال مسح الثغرات في توصيات لبناء نظم آمنة وفي تحصين النظم بالمعدات والبرمجيات المناسبة، وغلق الثغرات التي يمكن الآخرين من الدخول إلى النظام بطريقة غير مصرح بها، ولمن لا يملكون إذن الدخول.

2ـ **التفتيش العشوائي** (Random Checks)

من النظم الأمنية الجيدة التفتيش العشوائي دون سابق إعلام ودون تحديد وقت لذلك، ومن المفيد مراقبة الأشخاص الذين يتلصصون من وراء الكتف والظهر (piggybacking)، والذين لا يسمح لهم بدخول منطقة حساسة ما، الانتظار لحين وصول الشخص المعني ويلحقون به إلى المنطقة الحساسة.

3ـ **اختبارات الدخول غير المصرح به** (Penetration Tests)

يقوم بتنفيذ اختبارات فحص الدخول من قبل خبراء خاصة في المواقع الهامة (العكسرية، والذرية)، حيث يحاول فريق الخبراء تفحص الثغرات ومحاولة الولوج إلى النظام وإلى المناطق المحظورة.

أنموذج للحماية الفيزيقية للمعلومات

عندما يتم تقدير الأمن الفيزيقي لأي موقع بما في ذلك الحاسبات، فإن استخدام اتجاه الدائرة المركزية مناسب وقدم هذا الاتجاه على فكرة الانطلاق بشكل دائرة من أبعد موقع عن نقطة الأهمية (Point of interest) وقد تكون من موقف السيارات أو من الشارع المجاور للموقع والتحرك باقتراب وانتظام نحو تلك النقطة.

ولابد من معرفة وجود عوائق طبيعية (Natural Barriers) بين نقطة البداية وكل دائرة ونقطة الأهمية (الهدف)، وحواجز اصطناعية، وبهذه الطريقة يمكن تفقد كل دائرة من هذه الدوائر وتحديد نقاط الضعف والقوة في أمنها ومعالجة العيوب وفقاً لذلك (Icove, Seger, & VonStorch, 1995).

شكل رقم (5)
اتجاه الدائرة المركزية في الأمن الفيزيقي للمعلومات

المصدر: Icove, Seger, & VonStorcb, 1995, p. 107 مع التعديل

2ـ التشفير(التعمية) (Cyptography)

يحمي التشفير المعلومات الإلكترونية كما تحمي الأقفال المعلومات المطبوعة. وتتم الحماية بواسطة التشفير عن طريق خلط المعلومات الإلكترونية بحيث لا يمكن إعادة ترتيبها إلا باستخدام مفتاح معين، وتكون المعلومات المخلوطة غير مفهومة بتاتاً

لشخص لا يملك هذا المفتاح، وتعرف الرسالة المخلوطة بالرسالة المشفرة (Ciphertext). وتعرف عملية الخلط هذه بالتشفير (Encipherment or Encryption). أما عملية إعادة الرسالة الأصلية من الرسالة المشفرة إلى وضعها الأصلي فتعرف بعملية فك الشفرة (Decipherment or Decryption). كما تعرف طريقة معينة في التشفير وفك الشفرة بنظام التشفير (Cryptosystem) أو (Cipher). وتقوم كل نظم التشفيرعلى نوعين أساسيين من أنواع تحويل أو خلط الرسالة وهما: نقل الموقع (Transposition) والتبديل.

يعني نقل الموقع إعادة ترتيب موقع أو موضع النبضات أو الحروف في كلمات الرسالة. فيما يعني التبديل، تبديل النبضات، أو الحروف أو كتل النصوص ببدائل محددة. ويتم التشفير باستخدام طريقة رياضية محددة مع مفاتيح مختلفة. بحيث يكون ناتج استخدام نفس الطريقة مع المفاتيح المختلفة رسائل مشفرة مختلفة. ولفك الشفرة لابد من معرفة الطريقة والمفتاح المستخدمين في التشفير. وحيث إن المفتاح يبقى سرياً فإن الطريقة الرياضية المستخدمة تظل معلنة ومعلومة للجميع لإتاحة الفرصة للشركات المعنية لتطبيقها عملياً بتطويرالأجهزة والبرامج اللازمة لها.

والمثال التالي يبين تبديل موقع كمثال للتشفير حيث تقوم هذه الطريقة على تبديل حروف الرسالة على أساس كُتَل من خمسة حروف. والمفتاح لهذه الطريقة عبارة عن قائمة توضح أي حرف في الرسالة العادية يصبح الحرف الأول في الرسالة المشفرة وأي حرف في الرسالة العادية يصبح الحرف الثاني، والثالث، والرابع، أو الخامس. فالمفتاح (4، 3، 1، 5، 2) يعني أن الحرف الرابع في الرسالة العادية يصبح الحرف الأول في الرسالة المشفرة، والثالث يصبح الثاني والأول يصبح الثالث، والخامس يصبح الرابع، والثاني يصبح الخامس.

ومثال ذلك تشفير عبارة (مركز الدراسات والبحوث) نقوم أولاً بتقسيمها إلى مجموعات من خمسة أحرف كالآتي:

م ر ك ز أ   ل د ر ا س   أ ت و أ ل   ب ح و ث

ثم نقوم بتشفيرها باستخدام المفتاح أعلاه (4، 3، 1، 5، 2)، فتصبح كالآتي:

(زكمار   أرلسد   أوالت   ثوبح)

ولفك هذه الشفرة لابد من معرفة الطريقة والمفتاح السابق.

نقل الموقع: تقوم هذه الطريقة على تغيير موقع كل حرف للأمام في الرسالة الأصلية بعدد (س) موقع حرفي، على سبيل المثال فإذا طبقت هذه الطريقة باستخدام المفتاح (س= 3) على جملة (مركز الدراسات والبحوث) تصبح هذه الجملة كالآتي :

الحرف الأول م نغيّر موقعه ثلاثة مواقع حرفية للأمام حسب ترتيب الهجاء (أ ب ت ث ج . . . . ي) فتصبح الميم (و)، والحرف الثاني (ر) يصبح (ش)وهكذا. فتصبح عبارة (مركز الدراسات والبحوث)

(و ش ن ص ث هـ ز ش ث ض ث ح ب ث هـ ج ذ ب خ)

أي: (وشنص تهز شثضثح بثهجنج)

ولإعادة ترتيب الرسالة أي فك الشفرة تستخدم الطريقة والمفتاح في الحالتين للحصول على العبارة الأصلية.

نظام التشفير الرقمي (Digital Ciphers):

تم تطبيق نظم التشفير الحديثة في شكل رقمي باستخدام الحاسب الآلي والذي له مدخلان: الرسالة غير المشفرة والمفتاح وكلاهما ممثل تمثيلاً رقمياً في شكل سلسلة من الرقمين (0) و (1). أي باستخدام الترقيم الثنائي والحساب الثنائي وهي لغة الآلة في الحاسب الآلي.

ويتم التشفير بجمع كل رقمين ثنائيين أحدهما من الرسالة والآخر من المفتاح الذي هو عبارة عن سلسلة عشوائية ثنائية بطول الرسالة.

مثال ذلك إذا أردنا تشفير كلمة (CAB) باللغة الانجليزية التي تمثل الحروف رقماً كالآتي:

	B	A	C
كلمة (CAB)=	01000010	01000001	01000011
والمفتاح 1=	00101011	01111001	11010001
والكلمة المشفرة =	01101001	00111000	10010010

ويتم فك الشفرة بطرح الكلمة المشفرة والمفتاح ثنائياً. ويكون الجمع والطرح على أساس: 0+0=0، 1+0=1، 0+1=1، 1+1=0، وعادة فإن 1+1 = في الترقيم الثاني (10). وتسمى في المنطق الرياضي (XOR) أي (Execlusive OR)، أي يشمل أو وتكون نتيجة الـ XOR صفراً إذا كانت البايتات ذاتها [0 = 0 XOR 0]، و(1X0R1=1) وإذا كانت البايتات مختلفة [1= 0XOR1]، و(1X0R1=1)، ومن طرق التشفير المعروفة تشفير البيانات المعياري (DES)، وال(DES) الثلاثية، ومعايير التشفير المتقدم (AES) بالاضافة إلى (RC2)، و(RC4)، و(RC5).

فك الشفرة (Code Breaking):

هي العملية التي يتم بموجبها تحديد الرسالة الأصلية من الرسالة المشفرة بدون معرفة المفتاح السري المستخدم أو حتى الطريقة المستخدمة في التشفير. ويتضمن كسر الشفرة التحليل واستخدام طريقة الخطأ والصواب. والخطوة الأولى هي تحديد طريقة التشفير المستخدمة وطول المفتاح السري والذي يكون طوله من (40 إلى 128 بت (Bit)) (صفر أو واحد).

والخطوة الثانية هي تحديد المفتاح السري، وبعد ذلك يمكن كسر شفرة الرسالة. وإحدى طرق معرفة المفتاح السري باستخدام القوة الصرفة (Brute Force) لحاسبات عملاقة أو عدد كبير جداً من الحاسبات الشخصية لتجربة كل احتمالات المفاتيح في العثور على المفتاح الصحيح. وقد استخدمت هذه الطريقة لمعرفة المفتاح الصحيح وطوله (40 بت) باستخدام 120 محطة عمل وجهازي حاسب عملاقين Super) (Computer في مدة 8 أيام. كما تم معرفة المفتاح بعد ذلك باستخدام (209) كمبيوتر شبكي في (3.5) ساعة بسرعة اختبار (27) مليون مفتاح في الثانية. واستخدم طالب سويسري (7500) حاسب شخصي على الإنترنت في نفس الوقت لمعرفة المفتاح السري بطول (48 بت) وبسرعة 440 مليون اختبار مفتاح في الثانية، واستغرقت عملية معرفة المفتاح الصحيح (312) ساعة.

توليد وتوزيع المفاتيح (Generation & Distribution of Keys):

إن تصميم نظام تشفير قوي هو الخطوة الأولى نحو أمن المعلومات، ولكن بمستوى التحدي نفسه تكون إدارة المفاتيح (Key Management)والتي تشمل توليد أو انتاج المفاتيح وتوزيعها وتخزينها واسترجاع المفاتيح السرية.

وتستخدم لتوليد المفاتيح عمليات شبه عشوائية تشمل قراءة معلومات حالة النظام مثال ذلك وقت الساعة في جهاز الحاسب الآلي. وكلما كانت القيم هذه لا يمكن التنبؤ بها وتتغير بمستوى مناسب كلما صعب معرفة المفتاح بمراقبة نظام التشفير. مثال ذلك استخدام أرقام عشوائية مع وقت ساعة الحاسب ومعلومات أخرى عن حالة النظام لتوليد مفتاح عشوائي.

ولاستخدام التشفير لحماية الاتصالات لابد من طريقة يستطيع بها المرسل والمستقبل من الاتفاق على مفتاح سري، ومن البديهي أن المرسل لا يمكن أن يرسل المفتاح السري على قناة الاتصالات غير المشفرة، وهناك عدة حلول :

1ـ الاتفاق على مفتاح سري بالالتقاء شخصياً، وهذه غير عملية إذا كانا بعيدين جداً عن بعضهما.

2ـ شحن المفتاح السري عن طريق وسيط مأمون مثال ذلك إحدى شركات البريد السريع المأمونة. ولكن التأخير يجعل هذه الطريقة غير عملية.

3ـ الطريقة الثالثة هي استخدام طرف ثالث (شركة متخصصة) كوسيط مأمون، وتعطي هذه الشركة المتخصصة كل شخص مشتركاً بها مفتاحاً سرياً دائم يصله عبر البريد مثلاً.

وعندما يود أحد الأطراف ولنقل (أحمد) يريد أن يرسل رسالة لآخر ولنقل إلى (علي) فإن أحمد يطلب مفتاح للرسالة من الطرف الوسيط (الثالث وهو مركز المفاتيح) موضحا اسمه، واسم علي الذي يريد مراسلته.

ويقوم الوسيط بتوليد مفتاح عشوائي للرسالة يرسل نسخة منه مشفرة باستخدام مفتاح أحمد الدائم. بعد فك شفرة مفتاح الرسالة يقوم المرسل له باستخدام مفتاحه الدائم لتشفير الرسالة التي ينوي إرساله إلى علي. بعد ذلك ترسل الرسالة المشفرة إلى علي مع مفتاح الرسالة بعد تشفيره باستخدام مفتاح علي الدائم، والذي وصلها من قبل الطرف الوسيط. وعند استلام الرسالة يقوم علي بفك شفرة مفتاح الرسالة باستخدام مفتاحه الخاص الدائم. ثم يقوم باستخدام مفتاح الرسالة لفك شفرة الرسالة.

ويمكن أن تكون كل هذه الخطوات تلقائية بحيث لا يحتاج أحمد أوعلي للتعامل مع الوسيط (مركز المفاتيح) بل يقوم جهازاهما بكل العمليات أعلاه.

هذه الطريقة هي طريقة التشفير باستخدام المفتاح الخاص (Private Key Encryption)، ومن سلبياتها ضرورة وجود طرف مأمون ثالث (مركز المفاتيح)، وهو يمثل عنق زجاجة ومصدر تهديد للأمان، ولكن رغماً عن ذلك فإن الطريقة هذه قد استخدمت بنجاح كبير مثال ذلك البنوك.

تشفير المفتاح العام وآراس أيه (Public-key Cryptography and RSA)

1ـ التشفير بالمفتاح العام (PKIs)

التشفير يعني تحويل البيانات العادية (النص Plaintext) إلى صيغة رموز (Ciphertext)، ومن ثم إلى النص مرة أخرى باستخدام ما يسمى مفتاح، وعملية رياضية تسمى اللوغرائم (Algorithm). ويستخدم التشفير لإخفاء معلومات معينة وحماية المعلومات من التعديل، وحمايتها من الاستخدام غير المصرح به. والخطوة الهامة هي السرية الخاصة بالمفتاح المستخدم لأداء عمليات معينة، وليست محاولات حفظ اللوغرائم سرية، وذلك أن اللوغرثمات المستخدمة على الإنترنت في التشفير معروفة.

ويسمى احياناً أسلوب التشفير العام بالتشفير غير المتماثل (Asymetrci)، ويستخدم مفتاحين مختلفين، مفتاحاً عاماً، ومفتاحاً خاصاً. ويتم تكوين هذين المفتاحين من خلال معدات مثل البطاقة الذكية، أو برمجيات لدى المستخدم، أو تعطى للمستخدم من طرف موثوق. ويحفظ المستخدم أحد المفاتيح، ويتوافر الثاني لدى العامة من المستخدمين. إن معرفة المفتاح العام لا تعني معرفة المفتاح الخاص، ويتراوح طول المفتاح عادة من (512ـ1024) بايت.

ولنفرض أن شخصاً ما (أحمد) قد كون مفتاحاً عاماً له بحيث إن الراغبين بإرسال معلومات مشفرة له يتمكنون من ذلك، وبالتالي فإن أحمد يجعل من مفتاحه العام سهل الوصول من خلال إضافته إلى قاعدة بيانات على الشبكة. الأفراد الذين يرغبون بإرسال معلومات مشفرة لأحمد يسترجعون مفتاح أحمد العام، ويستخدمونه لتشفير المعلومات المرسلة له. وأحمد هو الشخص الوحيد القادر على قراءة المعلومات لأنه يملك المفتاح الخاص اللازم لفك التشفير، ولابد لأحمد من حفظ مفتاحه الخاص سرياً، وإلا فإن الآخرين يمكن أن يفكوا تشفير رسائله (GAO, 2001).

وفي حالة الوثائق الكبيرة الحجم، فيفضل أن يدمج المفتاح العام مع السري لتأمين طريقة فاعلة وفعالة في إرسال الوثائق المشفرة، وفي هذه الحالة يمكن تكوين مفتاح سري يسمى (مفتاح الجلسة)، ويستخدم لتفشير الوثيقة، ومن ثم يمكن استخدام المفتاح العام للشخص المرسل إليه لتشفير المفتاح السري للمرسل من خلال المفتاح العام لذلك الشخص (المرسل إليه)، ويرسل له المفتاح السري المشفر (مفتاح الجلسة) لفك تشفير الوثيقة.

أما في حالة البيانات كبيرة الحجم، فالحاجة ماسة إلى طريقة لخفض حجم البيانات المراد تشفيرها، ويمكن تحقيق ذلك من خلال اختصار البيانات، وتشفير البيانات المختصرة باستخدام المفتاح الخاص لتكون توقيعاً رقمياً، ومن ثم فك التشفير.

استخدم ديفي وهيلمان فكرة التشفير باستخدام المفتاح العام الذي يتيح الاحتفاظ بمفتاح لأمد طويل. وفي تشفير المفتاح العام كل شخص له مفتاح عام ومفتاح خاص به فقط، ويستخدمهما لفترة غير محدودة.

والمفتاح العام الذي يمكن ارساله عبر أي وسط غير آمن كالإنترنت ونشره بها ليكون معلوماً يستخدم للتشفير. بينما يستخدم المفتاح الخاص لفك التشفير، ولا يمكن حساب المفتاح الخاص رياضياً من المفتاح العام، فالعملية تكاد تكون مستحيلة تماماً. وتعرف هذه الطريقة باسم «تشفير المفتاحين»، و"التشفير اللامتماثل" (Asymetric Encryption)، أما الطرق التقليدية في التشفير والتي تستخدم مفتاحاً واحداً تسمى (تشفير المفتاح الواحد)، و(تشفير المفتاح الخاص)، و(التشفيرالمتماثل)، و(التشفير التقليدي).

2ـ طريقة آراس أيه

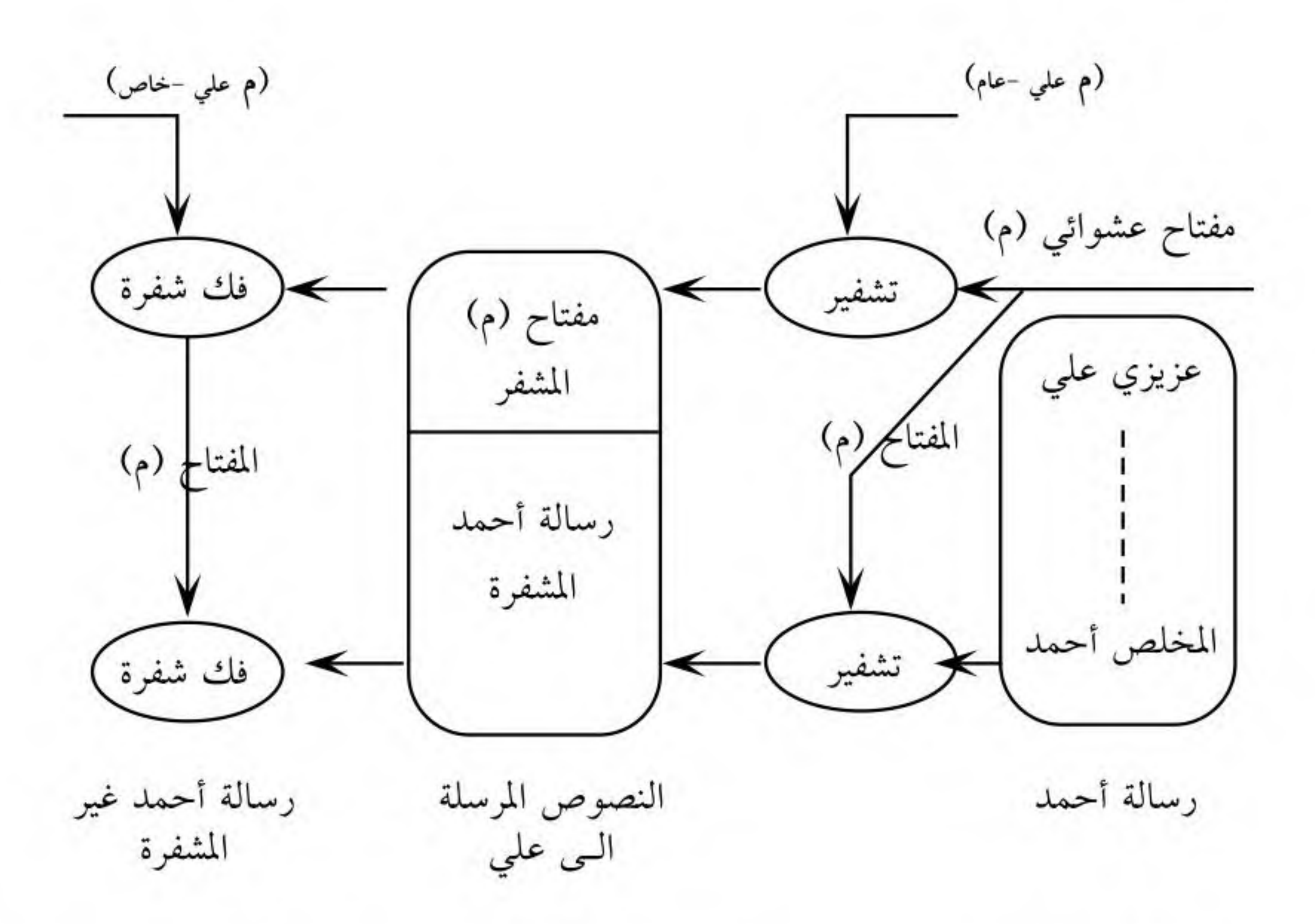
قام رولاند ريفست (Ronald Rivest)، وآدي شامير (Adi Shamir)، ولينارد آدلمان (Leonard Adleman) بابتكار وسيلة لتطبيق فكرة ديفي ـ هيلمان، وسميت هذه الوسيلة، أو الطريقة بنظام آر اس ايه (RSA)، وهي الحروف الثلاثة الأولى من أسمائهم الأخيرة. ونظام آر أس أيه يعمل كالآتي :

لإرسال رسالة عادية من أحمد إلى علي باستخدام نظام المفتاح العام (آر اس أيه) يقوم أحمد بتوليد مفتاح (م)[*] ويستخدمه لتشفير الرسالة بطريقة تشفير عادية مثل دي

---

* م = مفتاح   م – خاص = المفتاح الخاص، م عام = المفتاح العام.

إي أس (DES). في الوقت نفسه يقوم بتشفير المفتاح (م) باستخدام مفتاح أحمد العام (م) أحمد عام. وترسل الرسالة المشفرة، والمفتاح (م) المشفر إلى علي. فيقوم علي باستخدام مفتاحه الخاص (م) علي - خاص) لفك شفرة مفتاح الرسالة (م) واستخلاصه، ومن ثم يستخدم المفتاح (م) لفك شفرة الرسالة المرسلة، ويظهر الشكل التالي هذه العملية.



الشكل رقم (6) يوضح تسلسل عملية التشفير باستخدام مزدوج للمفتاح العام والخاص. (غيرت الأسماء إلى أسماء عربية)

المصدر : Denning, 2000 b, p. 302.

* م = مفتاح م - خاص = المفتاح الخاص، م عام = المفتاح العام.

3ـ توزيع المفاتيح العامة وديفي ـ هيلمان: (Public-key Distribution & Diffie-Hellman)

اخترعت هذه الطريقة للتغلب على مساوئ طريق (التشفير بواسطة توزيع المفتاح الخاص عن طريق طرف ثالث) والطرق الأخرى، وقد اخترعها ديفي وهيلمان الأمريكيين، وتقوم طريقتهما على فكرة زوج من مفتاح عام، ومفتاح خاص. وتبدأ الطريقة بأن يقوم كل طرف بتوليد مفتاح خاص بطريقة مستقلة. بعد ذلك يقومان بتوليد مفتاح عام عن طريق استخدام المفتاح الخاص أيضاً. ثم يقومان بتبادل المفتاحين العامين، ثم يقوم كل طرف بحساب دالة رياضية باستخدام المفتاح الخاص والمفتاح العام للطرف الآخر.

والعملية الرياضية تؤدى إلى أن تكون قيمتا الدالة لدى كل طرف متساويتين، وتستخدم هذه القيمة كمفتاح للرسالة. ولكي تكون هذه الطريقة آمنة يجب حساب المفتاح العام كدالة رياضية (احادية الاتجاه) من المفتاح الخاص. وإلا لأمكن لمتصنت يلتقط المفتاح العام أن يقوم بحساب المفتاح الخاص رياضياً منه وعندئذ يقوم بفك شفرة الرسالة. وتستخدم طريقة ديفي ـ هيلمان في عدة مراسم شبكات ومنتوجات اتصالات تجارية. وإحدى الصفات الجاذبة فيها أنه لا حاجة للاحتفاظ بالمفاتيح لأمد طويل، حيث يتم توليدها واستخدامها ثم رميها بعد انتهاء المحادثة أو الرسالة.

4ـ التشفير بالمفتاح السري

يستخدم أسلوب التشفير لضمان الموثوقية، وفي حالة التشفير بالمفتاح السري (يسمى أحياناً بالمفتاح المتماثل (Symmetric)، ويستخدم مفتاح واحد في التشفير (Encryption)، وفي فك التشفير (Decryption).

نظم المفتاح الخاص (المفتاح المتزامن أو المفتاحين).

ويتكون من مفتاح عام ومفتاح خاص، ويناسب هذا النوع في الشبكات و المؤسسات، حيث يكون لكل مستخدم مفتاح عام ومفتاح خاص (خاص بالفرد)،

الطريقة فقدان هذه البطاقات الذكية أو الكروت أو تلفها وبذلك يمكن أن تضيع مفاتيح التشفير ويستحيل فك شفرة البيانات. وإحدى الطرق لحل هذه المعضلة هي من خلال نظام استرجاع المفاتيح. وهو يؤمن إمكانية احتياطية لاسترجاع مفتاح التشفير. ويمكن إدارة هذا النظام من قبل الشخص أو المنشأة المستخدمة للتشفير أو إدارته بواسطة جهة ثالثة مستقلة ومؤتمنة (Trusted Third-Party).

تطبيقات التشفير: يمكن استخدام التشفير لحماية: (1) البيانات المخزنة بما في ذلك الملفات والأشكال داخلها، أو (2) الاتصالات، بما في ذلك المحادثات الهاتفية والفاكسات والبريد الإلكتروني ومعاملات الويب والمعاملات البنكية الإلكترونية واتصالات الجوال وتراسل الملفات (FTP) والعمل عن بعد (Telework).

ويتوفر التشفير عملياً في شكل أجهزة وبرامج، ويمكن الحصول عليه كأجهزة وبرامج مستقلة لحالها أو مضمن كصفة (Feature) في بعض المنتوجات. وهناك العديد من حزم البرامج والبرامج المساعدة تساند التشفير بما في ذلك حزم برامج تنسيق النصوص والجداول الإلكترونية وإدارة الملفات، وقواعد المعلومات، والمتصفحات، وبرامج البريد الإلكتروني، وهاتف الإنترنت. وتأتي برامج الحاسبات متضمنة التشفير بشكل متزايد. ويكون تشفير الاتصالات على نوعين:

1ـ تشفير من الطرف إلى الطرف (End-to -End).

2ـ تشفير الوصلة (Link Encrypted).

النوع الأول يوفر قناة آمنة بين الطرفين بغض النظر عن عدد الوصلات، أو الحاسبات الآلية التي تمر بها الرسالة. وتشفير الوصلة يحمي الرسالة خلال الوصلة الواحدة فقط، وليس كل المسار. وميزته أن كلا الطرفين لا يحتاجان لدعم التشفير أو لاستخدامها لنظم تشفير متوافقة والتشفير في الهاتف الجوال الدولي المستخدم في منطقة الشرق الأوسط (Global System for Mobile [GSM]) من هذا النوع. حيث إن الحلقة الضعيفة المعرضة للتصنت هي وصلة الهواء بين جهاز الجوال ومحطة الإرسال والاستقبال (محطة القاعدة).

ومن التطبيقات الهامة والآخذة في الأزدياد للتشفير استخدامه في الشبكات الافتراضية الخاصة (Virtual Private Networks) والمختصرة (VPNs). وهي شبكات

خاصة قليلة التكلفة باستخدام وسط عام (الإنترنت) بديلة عن الشبكات الخاصة التي تستخدم الخطوط المؤجرة العالية التكلفة (Leased Lines) لربط مواقع للمنشآت مترامية جغرافياً، وهي بذلك تمثل بديلاً قليل التكلفة، وتستخدم الإنترنت كوسط عام رخيص لعمل الشبكات الافتراضية الخاصة باستخدام أجهزة وبرامج خاصة بذلك.

هذا وقد تم تطوير العديد من المراسم الأمنية (Security Protocols) مثل (SSL)، و (SET) التي تستخدم التشفير والتحقق من الهوية لجعل الإنترنت وسطاً آمناً للاستخدامات التجارية والمالية والتبادلات المالية لبطاقات الائتمان غيرها.

قصور التشفير:

التشفير طريقة قوية لحماية البيانات أثناء إرسالها أو لحفظها في وسائط تخزين، ولكن لهذه الطريقة قصور في ناحيتين أساسيتين:

الأولى: أن التشفير لا يحمي البيانات أثناء معالجتها داخل الحاسب الآلي، حيث إن برامج المعالجة تتعامل مع البيانات غير المشفرة، لذلك فالبيانات عرضة للضرر بها في أي صورة من الصور أثناء معالجتها داخل الحاسب.

الثانية: أن التشفير ليس أفضل من أضعف وصلة في النظام، فمهما كانت متانة الرياضيات المبنى عليها فإن التطبيق العملي يصاحبه ثغرة ضعف في مكان ما يمكن أن يحدث منها الاختراق.

ورغماً عن أهمية التشفير القصوى في حماية البيانات إلا أنه لا يستطيع حمايتها ضد أغلبية الهجمات: فهو لا يستطيع حمايتها من الاستغلال والهجمات من داخل المنشأة من قبل الموظفين المتزمرين أوخداعهم واستجابتهم للخداع بحسن نية (الهندسة الاجتماعية)، كما لا يستطيع حماية البيانات ضد هجمات حصان طروادة (Trojan Horse)، أو الفيروسات، أو هجمات حرمان الخدمة (Denial of Service) وغيرها.

3ـ **المخابئ** (Steganography)

هو تخفية الرسائل في وسط ما كوثيقة أو صورة، أو تسجيل صوتي، أو فيديو. أي شخص يعلم أن هذا الوسط يحتوي على رسالة، ويعلم طريقة ترميز الرسالة داخل الوسط يمكنه استخراج الرسالة من الوسط. مثال ذلك خلال الحرب العالمية

الثانية قام أحد الجواسيس الألمان بإخفاء رسالة هامة داخل ما يبدو ظاهرياً مجرد تقرير صحفي عادي، وذلك بأن جعل كلمات التقرير الصحفي تبدأ بحروف الرسالة التجسسية المراد إرسالها.

بعض الأساليب المستخدمة الأخرى: الكتابة بالحبر غير المرئي، والصور الفوتغرافية المصغرة حتى حجم النقطة. وعند تكبيرها تظهر صفحة كاملة من المعلومات المطبوعة. وقد استخدمها الألمان الذين اخترعوا هذه الطريقة في إرسال المعلومات الاستخبارية في شكل نقاط على التلغرافات العادية وخطابات الغرام والمكاتبات التجارية. مثال آخر هو إخفاء الرسائل في الصور الملونة بترميزها رقمياً داخل النقاط الضوئية (Pixels) المكونة للصورة، وهناك برامج جاهزة كبرنامج أس ـ تولز (S-Tools) يقوم بذلك بكل سهولة، كما يمكنه تشفير الرسالة قبل اخفائها داخل الصورة. وهذه الطريقة تأخذ حجماً أكبر حيث يتضاعف حجم الرسالة عدة مرات لحجم الوسط المستخدم ولكن الميزة في درجة التخفي العالية حيث يمكن نشر صورة على الإنترنت للملأ ولن يعرف أنها تحتوى رسالة إلا القلة المراد لها أن تعرف. وقد استخدمت هذه الطريقة كذلك في الإنترنت لاخفاء نشاط إجرامي حيث قام أحد لصوص بطاقات الائتمان باخفاء أرقام البطاقات في صفحات ويب في موقع قام بالتعدي عليه ودخوله. ثم قام بتغيير علامات القوائم في الموقع (List Bullits) بصور ورسومات شبيهه ولكنها تحتوي على أرقام بطاقات الائتمان. ثم يقوم بعرض هذه الأرقام للبيع لعملائه الذين يقومون بالدخول للموقع وانزال الصفحات المعنية.

4ـ المجهوليه (الغفلية) (Anonymity):

هناك عدد من الأسباب التي تجعل الفرد غفلاً (غير مكشوف)من الهويته الحقيقية عندما يستخدم الإنترنت، فربما يريد أن يحمي نفسه ضد حكومة عدائية، أو أن يرسل رسالة على جماعات النقاش دون تعريف حقيقي لهويته، وهناك إخفاء بالتمويل للهوية على خادمات مثل (anon.penet.fi) أو إخفاء كتوم مثل (Mixmaster remailer) حيث يقوم على أخذ عنوان غير حقيقي في مكان ما، ويقوم ذلك الموقع بتحويل الرسائل إلى العنوان الحقيقي. أو إرسال الرسالة دون تحديد المرسل (الاسم أو العنوان). ويشترك مع بنت (Penet) أكثر من نصف مليون مشترك حيث يقوم بإعطاء كل مشترك رقماً خاصاً به حيث يتمكن الآخرون من مراسلته ومستوى الأمن فيه ضعيف لأنه لا يستخدم التشفير للرسائل.

يمكن تجنب بعض التهديدات الأمنية باتخاذ تدابير وافعال من غير الكشف عن الهوية، مثال ذلك شراء البضائع نقداً بدلاً عن بطاقات الائتمان، وكتابة رسائل غير موقعة في صناديق الاقتراحات وعمل المكالمات الهاتفية من تلفونات أو هواتف عملة، ويمكن احتجاب المعلومات الخاصة بشخص أو منظمة معينة حفاظاً على سرية هذه المعلومات.

وفي الإنترنت ظهر استخدام النقد الإلكتروني الرقمي (eCASH) للشراء دون إظهار الهوية، وهناك عدة أنظمة بعضها يتيح السرية التامة وبعضها يتيحها لحدود معينة. ومن أنظمة النقد الإلكتروني الرقمي نظام شركة ديجي كاش في هولندا.

يعرف مستخدمو الإنترنت الشبكة عن طريق مقدمي الخدمة وعن طريق عناوين بريدهم الإلكتروني، وإحدى الطرق لإخفاء الهوية هي استخدام خدمة إعادة إرسال البريد التي تقدمها بعض المواقع (Remailer) والذي يقوم بحذف المعلومات الشخصية منها وإرسالها للمرسل إليه الذي لن يعرف هوية الراسل. مثلاً إذا أراد أحمد إرسال رسالة إلى علي دون أن يعرف هويته يقوم بإرسال الرسالة إلى معيد إرسال البريد (Remailer) والذي يقوم بحذف معلومات الراسل ويقوم بعد ذلك بإرسالها إلى علي، وعند وصولها إلى علي سيعرف أن الرسالة أتت عن طريق معيد إرسال البريد ولكنه لن يعرف من أرسلها.

ويمكن استخدام أسلوب حجب الهوية (الشخصية) للأغراض المشروعة، أو الممنوعة. ومن الاستخدامات الإجرامية قيام أحد المبتزين إرسال رسالة غير موقعة عبر معيد إرسال رسائل يهدد فيها أن يطير طائرة صغيرة ذات تحكم عن بعد وإدخالها في ماكينة الطائرات النفاثة التي على وشك الإقلاع وذلك بأحد المطارات الألمانية بهدف إسقاط هذه الطائرات. وتمكن المحققون من معرفة معيد إرسال الرسائل وهي شركة أمريكا أون لاين، وتمكنوا من معرفة المبتز رغماً عن أنه كان يستخدم أسماء مستعارة لفتح حساب مع أمريكا أون لاين.

5ـ **الترشيح** (Sanitization) :

هي طريقة لعرض معلومات عامة منتقاة من معلومات سرية من غير الكشف عن المعلومات السرية الهامة نفسها، مثال ذلك تقوم إدارات الإحصاء السكانية بنشر

معلومات عامة إجمالية عن التعداد السكاني من غير الكشف عن معلومات تخص الأفراد والتي تعد سرية. وتقوم الشركات التجارية بنشر معلومات عامة عن منتوجاتها الجديدة من غير الكشف عن الأسرار الصناعية لديها. ويجب ألا تكشف الطريقة المستخدمة المعلومات السرية بحيث يمكن استنتاجها من المعلومات العامة المنشورة.

6ـ التخلص من النفايات المعلوماتية (Trash Disposal) :

إن التخلص السليم من وسائط المعلومات بما في ذلك استخدام آلة قص وتقطيع الأوراق يمكن أن يحفظ المعلومات الحساسة من المتلصصين الذين يعملون داخل المنظمة ويبحثون عن المعلومات الحساسة في صناديق النفايات بالمكاتب، أو ممن هم خارج المنظمة ويبحثون في مواقع النفايات الرئيسية للبلدة أو الحي. ولكن ليس كل تقطيع وقص يضمن سلامة المعلومات الحساسة، فقد أعلنت شركة ويكفيلد للتقنيات المدمجة بأمريكا عن تقنية تمكن من إعادة تركيب جزيئات الأوراق وترتيبها مرة أخرى.

أيضاً يحتاج التخلص من المعلومات الرقمية المخزنة في الحاسب الآلي، أو في أقراص مرنة أو ضوئية، أو شرائط مغنطيسية لعناية خاصة، فهناك برامج تستطيع أن تلتقط كلمات السر ومفاتيح فك الشفرة من داخل ذاكرة الحاسب الآلي، كما وهناك برامج وأساليب وطرق يمكن بها استرجاع البيانات من وسائط التخزين من بعد مسحها منها. ففي حادثة ومحاكمة فضيحة إيران قيت تمكن المحققون من استرجاع ثلاث رسائل بريد إلكتروني تمثل بينة مهمة في المحاكمة قام اوليفرنورث بمسحها من شرائط النسخ الاحتياطي بالحاسب الآلي بالبيت الأبيض الأمريكي.

7ـ درع المعلومات (Shielding) :

وهي إحدى الطرق لحماية المعلومات بالتغطية الحسية بمادة معينة كما في طائرات استيلث الحربية، وأقمار التجسس التي يتم تغطيتها بمادة معينة تمنع التقاط الاشارات المنعكسة من جسمها بواسطة الرادارات، وفي مجال المعلومات يمكن استخدام تقنية تمبست (TEMPEST) لإخفاء المعلومات عن طريق حجب الإشعاعات الكهرومغناطيسية الضعيفة المنبعثة من أي جهاز إلكتروني أو الحبل، فالشاشات وكيابل التلفونات والبيانات واللوحات الإلكترونية تشع إشعاعات ضعيفة كهرومغناطيسية يمكن التقاطها وتركيبها باستخدام تغطية تمبست. وهي باختصار حجب الإشعاعات الصادرة

من الأجهزة الإلكترونية والكيابل بوضعها داخل صناديق أو غرف حديدية، وهناك تقنيات أخرى في تمبست أكثر تعقيداً وكلفة لمنع هذه الاشعاعات من الانبعاث من دون وضعها في صناديق أو غرف حديدية وبذلك تتيح مزيداً من الحركة ولكنها مكلفة للغاية (Denning, 2000 b).

الفصل السادس عشر

نقاء المعلومات

مقدمة

يعني نقاء المعلومات (Authentication) العملية التي يتحقق بمقتضاها مدى أصالة ومصداقية المعلومات وتكاملها المتوفرة وأنها خالية من أي إفساد أو تزييف، ويشمل التحقق التأكد من أن الأشخاص أو العمليات داخل الحاسب، أو البرامج هي ما تدعى من شخصية وآليات لمعرفة إن كانت البيانات قد تم العبث بها أو اسندت إلى مصادر غير مصادرها.

وهناك أربع طرق تستخدم للتحقق من المصداقية، وهي :

أولاً: الصفات الشخصية، كالمظهر، والصوت، والخط.

ثانياً: سر من الأسرار مثل كلمات المرور، وأرقام التحقق الشخصية (PIN)، ومفاتيح فك الشفرة.

ثالثاً: حيازة شيء معين كالبطاقة الشخصية، أو كرت الدخول، أو كرت الائتمان، أورقم الهاتف.

رابعاً: الموقع، أو المعلومة. وكثير من طرق التحقق تستخدم وسائل مزدوجة من هذه الطرق لزيادة الموثوقية مثل استخدام المعلومات الشخصية (رقم التحقق الشخصي PIN) مع بطاقة البنك.

1ـ التحقق من الأمن الفيزيقي

هناك ثلاث طرق لفحص نظام الأمن الفيزيقي لموقع المعلومات، بدل الانتظار حتى حدوث تعدٍّ، وهذه الطرق هي :

1ـ تفتيش فيزيقي منتظم وذلك على أساس منتظم.
2ـ تفقد عشوائي، وذلك للتأكد من الموظفين لا يخترقون إجراءات الأمن الفيزيقي عندما يعتقدون أن لا أحد يراقبهم.
3ـ اختبارات الاختراق، وذلك في المواقع الأكثر حساسية.

ومن إجراءات السلامة المتعلقة بالكوارث الطبيعية المتعلقة بالمعلومات استخدام منبهات الحريق والدخان، ووضع حواجز للكوابل وخطوط المياه وإبعادها وعزلها عن غرفة المعلومات، والتأكد من نظام التنبيه للحريق يقوم تلقائياً بإغلاق أنظمة التبريد والحاسب، وإبعاد المياه (القوارير) والمواد السامة . . . إلخ. واستخدام سياسة عدم التدخين لإبعاد التدخين عن الحاسب ولتجنب الحرائق، وإبعاد المعدات المتعلقة بالحاسب غير المستخدمة في مكان آمن.

وأخيرا وفيما يتعلق بالداخلين المتطفلين (Intruder) فيجب أخذ الحيطة اللازمة حول غرفة المعلومات، والغرف التي تستخدم لتخزين مواد المعلومات، وتحصين غرفة المعلومات بحيث لا يمكن من تسلقها والدخول إليها، وأن الفيضانات الخاصة بالتهوية أو التبريد صغيرة بحيث لا يمكن الفرد من دخولها، ولقد حددت دايننج (Denning. 2000b) الوسائل التالية في فحص أصالة المعلومات.

2ـ وسائل الكشف والإثبات البيولوجية الاحصائية (Biometrics) :

كان الناس يبرهنون عن شخصياتهم ومصداقيتهم لبعضهم بعضاً عن طريق المظهر الخارجي للصوت، ويعتمدون في ذلك على الذاكرة والوصف الذي يقدمه الآخرون للتعرف على الشخص المعني. وبعد اختراع التصوير الفوتغرافي أمكن تسجيل المظهر الخارجي بالصورة، وبعد اكتشاف البصمة (Fingerprint) أمكن التعرف على الشخص الذي لا مس الأشياء الموجودة في مسرح الجريمة باستخدام بصمة الأصابع. وبعدها جاءت بصمة الحامض النووي (DNA) لتقدم طريقة دقيقة في مقارنة الأدلة في مسرح الجريمة وخاصة في جرائم القتل، والاغتصاب، ثم تطور الأمر مؤخراً حيث استخدمت بصمة الحامض النووي (DNA) في الاثبات، وقد استخدمت هذه الوسيلة لدقتها ليس فقط في إدانة مرتكبي الجرائم، وإنما في إطلاق سراح كثير من الذين أدينوا عن طريق الخطأ في جرائم القتل والاغتصاب. ويكفي أن نذكر أنه منذ عام (1988)، وهو العام الذي استخدمت فيه بصمة الحامض النووي أو البصمة الوراثية (DNA) في المحاكمات ومن بينها محاكمة أوجي سمسون (OJ Simson) الشهيرة في الولايات المتحدة ـ فإن هذه الوسيلة قد استخدمت في أكثر من (30.000) حالة، وأن نسبة الخطأ فيها حوالي (1) إلى (200) مليون. ويمكن أن تستخدم هذه الطرق في كشف الهوية، وإثبات الهوية، ومن عيوبها أنها غالية الثمن.

3ـ قياس التمامية (التكاملية) (Integrity Checksum) :

قد يكون من المستحيل في بعض الحالات منع أي إنسان أو برنامج من العبث بالمعلومات كأن يتمكن شخص متطفل أو فيروس من الدخول بصورة غير قانونية لملفات الحاسب الآلي وتعديل محتوياتها. ويبقى أفضل شيء في مثل هذه الحالات هو معرفة إن كان قد تم أي تعديل للبيانات، ويتم ذلك عن طريق قياس مصداقية وسلامة المعلومات.

ويكون قياس المصداقية والسلامة بحساب قيمة معينة مستخرجة من البيانات المراد حمايتها، ويتم تخزين هذه القيمة مع البيانات نفسها في موقع معلوم أو يتم تخزينها في مكان آخر، وعندما يراد قياس مصداقية وسلامة البيانات يتم حساب هذه القيمة مرة أخرى، ويتم مطابقة القيمة الجديدة مع القيمة المخزنة، فإن تطابقا كان ذلك دلالة على أن البيانات لم يتم العبث بها.

4ـ التوقيع الرقمي (Digital Signature) :

لقد تمخض عن اختراع التشفير باستخدام المفتاح العام أمران مهمان: أولهما إمكانية إرسال الأسرار لطرف آخر بدون الحاجة إلى قناة أخرى لإرسال مفتاح الشفرة أو طرف ثالث موثوق به، والأمر الثاني إمكانية استخدام التوقيع الرقمي.

والتوقيع الرقمي هو عبارة عن كتلة بيانات مرفقة مع الرسالة أو الوثيقة ويربط الرسالة بمصدر شخصي أو جهة معينة. ويمكن التحقق من الشخص أو الجهة بواسطة المستلم، أو جهة محايدة ثالثة. والتوقيع الرقمي يؤكد مصداقية المصدر. فإذا احتوت الكاميرا الرقمية على المفتاح الخاص لصورة (لتوقيعها) عندما التقطت، يمكن أن يكون التوقيع إثباتاً قوياً بأن تلك الصورة قد التقطت بتلك الكاميرا، مما يكشف أي عملية انتقاء وتعديل في الصورة والتي من السهل عملها.

5ـ كلمات المرور والمتعلقات السرية الأخرى(Passwords & Other Secrets) :

تعتمد العديد من أنظمة التحقق والتحكم في الدخول على معلومة سرية مثل الأرقام المتعددة للخزائن الحديدية وشفرات فتح الأبواب وكلمات المرور، وأرقام

التعريف الشخصية (PIN). هذه المعلومة السرية يمكن حفظها في الذاكرة البشرية، أو في أداة تخزين كشارة دخول، أو كرت، أو قرص حاسب آلي.

كلمات المرور الشائعة الاستخدام يمكن معرفتها بواسطة برامج تستخدم القوة المطلقة (Brute Force) عن طريق تجربة كل كلمات القاموس مثلاً. ولتأمينها يجب أن تكون كلمة المرور على الأقل بطول (9) حروف وليست مماثلة لكلمة في القاموس وتحتوى على حرفين غير حروف الهجاء، أو الأرقام، وكما وهناك بعض البرامج التي تستطيع كشف كلمات المرور أثناء إرسالها عبر الشبكة إن لم تكن مشفرة. وللحماية القصوى لكلمات المرور تستخدم كلمات المرور لمرة واحدة فقط ثم تتغير، وهناك عدة نظم تستخدم التوقيع الرقمي على أنه برهان لا يستطيع مرسل الرسالة إنكار أنه لم يرسلها (Non-repudiation). فما لم يفرط المرسل في مفتاحه الخاص لا يمكن أن تكون قد أرسلت من طرف آخر. ويستخدم التوقيع الرقمي مع التشفير لتوفير الحماية اللازمة والموثوقية لأنظمة البريد الإلكتروني وبرامج الاتصالات لتبادل البيانات الحساسة وفي التجارة الإلكترونية.

6ـ إدارة المفاتيح العامة والشهادات (Public-key Management & Certificates):

تم اختراع التشفير باستخدام المفتاح العام لحل معضلة إدارة وتوزيع المفاتيح الخاصة في النظام السابق له، ولكنه في سياق ذلك أدى لظهور مشكلة أخرى هي المفاتيح العامة المزورة التي تستخدم لانتحال شخصية أخرى، وبذلك تستلم وترسل رسائل باسمه. هذه المشكلة تم حلها بشهادات المفاتيح العامة (بي كي آي PKI)، وهي شهادات رقمية تصدر بواسطة جهات موثوقة وتبرهن على مصداقية المفتاح العام، والمالك له، ومن هذه الجهات شركة (Verisign) العالمية وغيرها من الشركات المتخصصة في هذا المجال.

7ـ العلامات المائية (Watermarks) :

العلامة المائية هي رسم يدخل على الوثيقة، أو الصورة، أو الفيديو، أو التسجيل الصوتي، بمنشأ الرسالة، ويخدم عدة أهداف منها إثبات الملكية ومحاربة التزييف، وإثبات سلامة الوثيقة. فالعلامة المائية في العملة الورقية مثلاً تستخدم كبرهان على أن

هذه العملة قد صدرت من جهة معتمدة. وقد لا ترى العلامة المائية بالعين المجردة، أو لا تسمع بالأذن في حالة الوسائل السمعية. وفي هذه الحالة يجب استخدام وسائل خاصة للتعرف على هذه العلامة المائية حتى يمكن الاطمئنان إلى مصداقية الوثيقة ومصدرها.

8ـ الاتصال الراجع والاتصال بالمنزل (Call Back & Call Home):

تساعد آليات الاتصال الراجع في القيام بالحراسة ضد منتحلي الشخصية عن طريق الاتصال بالخط الهاتفي العادي. وذلك أنه متى ما اتصل شخص بنظام الحاسب الآلي يسأل النظام عن اسم المستخدم ثم يتعرف على رقم هاتفه من خلال البحث في قاعدة المعلومات المعتمدة والمخزنة لدى النظام، ثم يتصل الحاسب الآلي بالشخص المعني به في ذلك الرقم لإكمال عملية التحقق من الشخصية والولوج للنظام. وعلى هذا الأساس فإن منتحل الشخصية لا يتستطيع أن يستفيد من معرفته اسم الحساب، وكلمة السر التي تخص المنتحل شخصيته حيث إن الاتصال الراجع لا يتم إلا لرقم هاتف المستخدم الأصلي وليس رقم المنتحل.

فهذه الطريقة تستخدم للتحقق من مصداقية خط الهاتف وبالتالي مصداقية المتصل، وتستخدم طريقة مماثلة في الإنترنت للتحقق من شخصية المشتري، أو طالب الخدمة بإرسال بريد إلكتروني على العنوان المسجل بقاعدة بيانات موقع الخدمة يطلب تأكيد الطلب. وللحد من سرقة الحاسبات المحمولة تستخدم بعض البرامج التي تقوم بالاتصال آلياً بموقع معين كل فترة زمنية، فإن سُرِق الحاسب المحمول أمكن التعرف على مكانه من رقم الهاتف المتصل فيه.

9ـ التحقق بناءً على الموقع:

من مشاكل الفضاء الافتراضي (Cyberspace) في الإنترنت عدم معرفة المواقع الجغرافية للأطراف المتصلة، أو المتعاملة تجارياً، وقد أدى ذلك لصعوبة تتبع مجرمي العالم الافتراضي، ومعرفة مواقعهم الجغرافية، وخاصة عند مرورهم بعدة أجهزة كمبيوتر ومواقع.

إن التحقق من الشخصية بواسطة الموقع الجغرافي هو إحدى الوسائل المتاحة،

وبذلك لا يستطيع متطفل من روسيا الدخول إلى بنك في الولايات المتحدة الأمريكية منتحلاً شخصية صاحب حساب في الأرجنتين.

ويتسخدم في هذا النظام المعلومات الجغرافية التي تبثها مجموعة مكونة من (24) قمراً صناعياً يتم بواسطتها التحديد الدقيق للموقع الجغرافي بواسطة جهاز خاص يلتقط هذه الإشارات. ويقوم جهاز المتصل بإرسال هذه المعلومة للحاسب الرئيس الذي يقوم بمضاهاة هذه المعلومة مع البيانات المخزنة لديه.

10ـ الشارات والبطاقات (Badges & Cards) :

هناك العديد من وسائل التحقق يمكن استخدامها بالتلازم مع البطاقات البلاستيكية أو أية شارات أخرى يمكن استخدامها للتحكم في الدخول إلى المباني، والغرف، وأجهزة الكمبيوتر، والحاسبات البنكية، ومصادر المعلومات الأخرى، ومثال ذلك التوثيق الرقمي، والمعلومات البيولوجية. والبطاقات ذاتها يمكن أن تحتوي على معلومات كالاسم، والعنوان، ورقم الحساب، والمعلومات الطبية، وصلاحيات الدخول إلى غير ذلك. وتخزن هذه المعلومات على البطاقات في شكل (رموز قضبان) (Bar Codes)، أو في شريط ممغنط، أو في شريحة إلكترونية على البطاقة.

المراجع العربية

ابراهيم، حسنين توفيق (1997) . الأمن في عالم متغير . مجلة الفكر الشرطى، 6(3) ، 173-943 .

ابراهيم، حسنين توفيق (1998) الإنترنت والأمن : تحديات جديدة على مشارف القرن القادم . مجلة الفكر الشرطى، 7(2) ، 771-391 .

الاعسم، علي (1997). عوامل انجاح شبكة انترنت عربية: تقنية، تخطيط، استثمار. المستقبل العربي8، 93-100 .

الألفي، رمضان (1997). رؤية خاصة لأفاق الاستراتيجية الأمنية لدخول القرن الواحد والعشرين. مجلة مركز بحوث الشرطة، (21) ، القاهرة.

الأيام (1999). الولايات المتحدة تطلق الإنترنت ٢ للألفية القادمة. صحيفةالأيام، 8463 .

البحر، عبد الرحمن (1999). معوقات التحقيق في جرائم الانترنت. "رسالة ماجستير غير منشورة" . الرياض : أكاديمية نايف العربية للعلوم الأمنية.

البداينة، ذياب (1997أ) جرائم الحاسب الدولية. ورقة قدمت في ندوة جرائم الحاسب. معهد التدريب: أكاديمية نايغف العربية للعلوم الامنية. الرياض. السعودية.

البداينة ، ذياب (1997ب). شرطة المجتمع : أنموذج لعمل الشرطة العربية المستقبلي مجلة الفكر الشرطى الصادرة عن شرطة الشارقة، 6(3) ، 311-921 .

البداينة، ذياب (1988أ). الأمن الوطني في عصر المعلومات. صحيفة الجزيرة السعودية الاعداد (9421, 9428, 9435, 9442).

البداينة، ذياب (1998ب). الجرائم المستحدثة والبحث العلمي في المجتمع العربي. بحث مقدم للندوة العلمية حول دور البحث العلمي في معالجة مشكلة الجريمة والإنحراف في الدول العربية. أكاديمية نايف العربية للعلوم الأمنية، الرياض ، السعودية .

البداينة، ذياب (1998ج). التقنية والاجرام المنظم. ورقة قدمت في الندوة العلمية(47) الجريمة المنظمة واساليب مواجهتها في الوطن العربي. الاسكندرية 18-1998/20. أكاديمية نايف العربية للعلوم الأمنية،

البداينة، ذياب (1999أ)، جرائم الحاسب والانترنت، ورقة مقدمة في الندوة العلمية «الجرائم المستحدثة في الوطن العربي»، تونس، أكاديمية نايف العربية للعلوم الأمنية.

البداينة ، ذياب (1999ب). التطبيقات الإجتماعية للإنترنت . بحث مقدم للحلقة العلمية حول شبكة الإنترنت من منظور أمني، أكاديمية نايف العربية للعلوم الأمنية، بيروت، لبنان

البداينة، ذياب (2000). التحديات القامة للمجتمع العربي. مجلة دراسات مستقبلية، ع 5،

ص ص 87-100.

البداينة، ذياب (2005أ). الاردهاب الالكتروني. ورقة مقدمة في الدورة التدريبية الإعلام والارهاب. نظر: جامعة نايف العربية للعلوم الأمنية.

البداينة، ذياب (2005أ). الأمن الوطن في عصر العولمة، عمان: المجلس الأعلى للشباب.

البدر، بدر حمود، والزومان عبدالعزيز حمد (1997). ضبط استخدام الانترنت: لماذ وكيف. المؤتمر الوطني الخامس عشر للحاسبات الالية. جامعة الملك فهد للبترول والمعادن، وجمعية الحاسبات السعودية، 17-1997/10/19.

البشرى، محمد الأمين، والبداينة، ذياب (1999) أنموذج تصوري للمناهج الدراسية في الكليات الأمنية لتلبية الاحتياجات الأمنية في القرن الحادي والعشرين. الرياض : مركز الدراسات والبحوث، اكاديمية نايف العربية للعلوم الأمنية

البنك الدولي. (1998). تقرير التنمية البشرية. مؤشرات التنمية في العالم. القاهرة: MeRic

الحمادي ، صالح (1998). الشرطة والتحديات المستقبلية في مواجهة الجريمة ، مجلة الأمن الصادرة عن شرطة دبي ، السنة32 (872)، 84-35.

الخطيب ، محمود (1997). الصراع بين الإباحية والفضيلة على الإنترنت ، المجتمع، (1247)، 14-20.

الخليفة، عمر (2000) علم النغس والمخابرات. بيروت: المؤسسة العربية للدراسات والنشر.

الخميس، عبدالعزيز (1997). الانترنت أصبحت عربية. المجلة. ع 884، 1997/1/25، ص3-6.

الريس، نزار (1986). البحث العلمي في إسرائيل في الأبعاد التربوية للصراع العربي الإسرائيلي. وقائع المؤتمر العلمي، كلية التربية، جامعة الكويت ومركز دراسات الوحدة العربية : بيروت : مركز دراسات الوحدة العربي.

الشهاوي، قدري عبدالفتاح (1998). المنظومة الأمنية والآثار السلبية والإيجابية لشبكة الإنترنت. مجلة الفكرالشرطي، 7(2) ، 561-471.

الشوا ، محمد سامي (1994). ثورة المعلومات وانعكاسها على قانون العقوبات . القاهرة : دار النهضة العربية.

الصغير، جميل عبدالباقي (1992) . الجرائم الناشئة عن استخدام الحاسب الآلي . القاهرة : دار النهضة العربية .

العامر، محمد (1999). فيروس تشيرنوبل يغزو البحرين. صحيفةالأيام ، 6073.

العبيدلي ، عبيدلي (1998). الإنترنت وسيلة تدريب كفؤة ، آفاق العلم والمجتمع (23)، 6-7.

العليوي، ابو القاسم (1984). التربية والتكنولوجيا ومستقبل العرب. المستقبل العربي، 66 (8). بيروت : مركز دراسات الوحدة العربية. 48-61.

العمر، معن خليل، (2001) قضايا اجتماعية معاصرة. العين: دار الكتاب الجامعي

العور ، منصور محمد عقيل، وقاسم،علي (1996). الإنترنت والأبعاد الأمنية . ورقة مقدمة للحلقة النقاشية حول الإنترنت من منظور أمني ، القيادة العامة لشرطة دبي، دبي، الإمارات العربية المتحدة.

الفايدي، محمد عوض (1998). معوقات استخدام البحوث العلمية في معالجة المشكلات الأمنية. "رسالة ماجستير غير منشورة". الرياض: أكاديمية نايف العربية للعلوم الأمنية.

القاسم، صبحي (2000). مسيرة البحث العلمي والتطوير في الوطن العربي: معالم الواقع وتحديات المستقبل. شؤون عربية، 104، 136-160.

القاسم، صبحي (1999). نظم البحث والتطوير في البلدان العربية : واقعها والالتزامات الجديدة لتقديمهـــــا "ورقة مقدمة في مؤتمر التعليم العالي والبحث العلمي لمواجهة تحديات القرن الواحد والعشـــــرون". الرياض 17-1999/4/21 .

الكاملي، عبدالقادر (1998). التجارة الالكترونية العربية حاضراً ومستقبلاً. انترنت، 1 (8) مايو. ص ص 20-34.

الكمبيوتر (1997). إسرائيل تهاجم الكويت عبر الإنترنت ، الكمبيوتر والإتصالات والإلكترونيات ،(10)، 48.

المؤتمر الاقليمي العربي حول التعليم العالي (1998). اعلان بيروت حول التعليم العالي. بيروت : المؤلف.

المحيلان ، عبدالرحمن صالح (1998) . كلمة المقدمة ، مجلة آفاق الإنترنت، السنة1 (7)، 6.

النعيمي، طه، ونعمان النعيمي (1999). آليات تسويق نتائج البحث العلمي لخدمة التنمية والمجتمع. "المؤتمر السابع للوزراء المسؤولين عن التعليم العالي والبحث العلمي في الوطن العربي". الرياض، 17-1999/4/21.

أوينز، وليم: ادارة السياسة الدفاعية في القرن الحادي والعشرين ص ص 85-110 في مركز الامارات للدراسات والبحوث والاستراتيجية (2001) القيادة والادارة في عصر العولمة. أبو ظبي: المؤلف.

ايليوت كوهين: ادارة الامن القومي في عصر المعلومات ص ص111-140 قي مركز الامارات للدراسات والبحوث والاستراتيجية (2001) القيادة والادارة في عصر العولمة. أبو ظبي: المؤلف.

بكري، سعد الحاج (1991). شبكات الاتصال وتوظيف المعلومات في مكافحة الجريمة . المجلة العربية للدراسات الأمنية والتدريب 11، 11-32.

بلقزيز عبدالإله، (2000) نهاية الداعية: الممكن والممتنع في ادوار المثقفين. بيروت: المركز

الثقافي العربي
تميم، ضاحي (1996). الانترنت: رؤية أمنية. بحوث ودراسات شرطية. مركز البحوث والدراسات شرطة دبي.
جاد، نبيل، (1999). جرائم الحاسب الالي. بحوث ودراسات شرطية شرطية. ع89. مركز البحوث والدراسات. شرطة دبي، دبي.
جارنم، ديفيد (1998). أساسيات الأمن القومي : تطبيقات على دولة الامارات العربية المتحدة. أبوظبي : مركز الامارات للدراسات والبحوث الاستراتيجية.
جاسم ، صلاح خليفه ، ومعروف ، نزار (1996) . الدليل العربي الشامل لشبكة الإنترنت. البحرين : دار الهلال .
جبور، سمير (1982). العلم والتكنولوجيا في اسرائيل (80-81). بيروت: موسسة الدراسات الفلسطينية.
جعفر ، فهد عبدالكريم (1997). شبكة الإنترنت : محتوياتها وطريقة عملها . بحث مقدم إلى الإجتماع الخامس للجنة المتخصصة بالجرائم المستجدة، ، مجلس وزراء الداخلية العرب ، تونس، 7-9 يوليو 1997 .
جعفر، فهد عبدالكريم (1997). شبكة الانترنت: محتوياتها وطريقة عملها. الفكر الشرطي 6(4) 243-268.
جيتس بيل (1995-1998) طريق المستقبل. ترجمة عبدالسلام رضوان. الكويت: عالم المعرفة.
حجازي، سهير(1999). التهديدات الاجرامية للتجارة الالكترونية. بحوث ودراسات شرطية. ع91. مركز البحوث والدراسات. شرطة دبي، دبي.
حسين، سمير محمد (1996). مستقبل النشر الالكتروني العلمي. المجلة العربية للدراسات الانسانية. 14 (56)، 288-302.
خليل ، عزة محمود أحمد (1994) . مشكلات المسؤلية المدنية في مواجهة فيروس الحاسب دراسة في القانون المدني والشريعة الإسلامية . القاهرة : لايوجد ناشر .
داود، حسن طاهر (1997). أمن المعلومات. ورقة قدمت في ندوة جرائم الحاسب. معهد التدريب: أكاديمية نايغف العربية للعلوم الامنية. الرياض. السعودية.
راثمل، اندرو، (1998). الارهاب عبر الانترنت. ترجمات شرطية. ع 84. مركز البحوث والدراسات. شرطة دبي، دبي.
راثمل، اندرو، (1999). الجريمة في فضاء الانترنت. ترجمات شرطية. ع86. مركز البحوث والدراسات. شرطة دبي، دبي.
رستم ، هشام محمد فريد (1994). الجوانب الإجرائية للجرائم المعلوماتية دراسة مقارنة.

أسيوط : مكتبة الآلات الحديثة.

رسمي ، محمد حسن (1997) . تحديات القرن الواحد والعشرين والمواجهة. مجلة الفكر الشرطي ، (3) ، م6 ، شرطة الشارقة

رضا، محمد جواد (1998). العرب في القرن الحادي والعشرين: تربية ماضوية وتحديات غير قابلة للتنبؤ. . المستقبل العربي4، 47-63.

زحلان، انطوان (1990). العلم والسياسات العلمية في الوطن العربي. بيروت : مركز دراسات الوحدة العربية.

زحلان، أنطوان (1985). الانتاج العلمي العربي في إعداد الوب للانتاج العلمي. بيروت : مركز دراسات الوحدة العربية.

سلمان، سعيد (2000). مشروع التعاون العربي الأوروبي في مجال البحث. "ورقة مقدمة في ندوة البحث العلمي في العالم العربي وآفاق الألفية الثالثة : علوم وتكنولوجيا". الشارقة 24-2000/4/26.

سليم، طارق عبدالوهاب (1997). الجرائم المرتكبة بواسطة الانترنت وسبل مكافحتها. بحث مقدم إلى الاجتماع الخامس للجنة المتخصصة بالجرائم المستجدة. تونس. 7-1997/7/19م.

سنو، مي العبدالله (1998). العرب في مواجهة تطور تكنولوجيا الاعلام والاتصال. المستقبل العربي 4، 32-46.

شاهين، بهاء (1996). شبكة الإنترنت . القاهرة : العربية لعلوم الحاسب كمبيوساينس.

شعبان، مصطفى (2000). حجم الانفاق والقوى البشرية العاملة في البحث والتطوير في العالم العربي وآفاق الألفية الثالثة. "ورقة مقدمة في ندوة البحث العلمي في العالم العربي وآفاق الألفية الثالثة : علوم وتكنولوجيا". الشارقة 24-2000/4/26.

شهاب الدين، عدنان (1998). رؤية كلية لدور العلم والتكنولوجيا ودور مراكز البحث العلمي في خطط التنمية. "ورقة مقدمة في مؤتمر البحث العلمي والتطوير التكنولوجي ودورها في تعزيز القدرة التنافسية للقطاع الصناعي في دول مجلس التعاون الخليجي. البحرين.

طعم الله، خميس (1981). العرب في السنة 2000. شؤون عربية (1). جامعة الدول العربية. 127-142.

طلبه ، محمد فهمي وآخرون (1996) . الإنترنت. . طريق المعلومات السريع . القاهرة : مجموعة كتب دلتا .

عابدين، عبد الإله (2000). مشاكل البحث العلمي عند العلماء الشباب في العالم العربي.

"ورقة مقدمة في ندوة البحث العلمي في العالم العربي وآفاق الألفية الثالثة : علوم وتكنولوجيا" . الشارقة 24-2000/4/26 .

عبادة، عبادة، (1999). التدمير المتعمد لانظمة المعلومات الالكترونية. بحوث ودراسات شرطية شرطية. ع 87. مركز البحوث والدراسات. شرطة دبي، دبي.

عدس ، عمر حسن (1995) . جرائم الحاسب الآلي: أشكالها وأساليب مواجهتها. بحث مقدم للمؤتمر التاسع عشر لقادة الشرطة والأمن العرب ،مجلس وزراء الداخلية العرب، تونس، 61-81 أكتوبر 1995م.

عكاشة، سعد الدين (1999). تمويل البحث العلمي في الوطن العربي وسبل تنميته. "ورقة مقدمة في مؤتمر التعليم العالي والبحث العلمي لمواجهة تحديات القرن الواحد والعشرون" . الرياض 17-1999/4/21 .

علي، نبيل (2001). الثقافة العربية وعصر المعلومات. عالم المعرفة، 276. الكويت : المجلس الوطني للثقافة والفنون والآداب.

علي، نبيل (1994). العرب وعصر المعلومات. عالم المعرفة، 184. الكويت : المجلس الوطني للثقافة والفنون والآداب.

فليبسون، ستيفن (2000) الجريمة الالكترونية في القرن ال21. ترجمات شرطية. ع 100. مركز البحوث والدراسات. شرطة دبي، دبي.

قناة الجزيرة في قطر (199). حصاد اليوم، 1999/4/1 .

كاكو، ميتشو، ترجمة سعد الدين خرفان، (2001). رؤى مستقبلية. الكويت: عالم المعرفة 270

كريستيان كروملیش (1996) . ألفباء الإنترنت .(مركز التعريب والبرمجة بالدار العربية للعلوم ، مترجم).بيروت : الدار العربية للعلوم (تاريخ نشر العمل الأصلي غير موجود) .

كليش، فرانك (2000). ثورة الانفوميديا : الوسائط المعلوماتية وكيف تغير عالمنا وحياتك ; ترجمة حسام الدين زكريا، الكويت : عالم المعرفة، (253).

كمال، مروان، وزيدان كفافي (2000). البحث العلمي المؤسسي : الجامعات الرسمية الأردنية. "ورقة مقدمة في ندوة البحث العلمي في العالم العربي وآفاق الألفية الثالثة: علوم وتكنولوجيا" . الشارقة 24-2000/4/26 .

كون، توماس (1992/1968) بنية الثورات العلمية. ترجمة شوقي جلال. الكويت: عالم المعرفة.

لجنة إدارة شؤون المجتمع العالمي (1995). جيران في عالم واحد. ترجمة مجموعة من

المترجمين. الكويت : عالم المعرفة.

مجلس وزراء الداخلية العرب(1983). الاستراتيجية الأمنية العربي. تونس : الأمانة العامة لمجلس وزاء الداخلية العرب.

مراياتي، محمد (1999). دعم جهود البحث العلمي والتطوير في المعلوماتية. "ورقة مقدمة في مؤتمر التعليم العالي والبحث العلمي لمواجهة تحديات القرن الواحد والعشرون". الرياض 1999/4/21/17.

مركز الامارات للدراسات والبحوث والاستراتيجية (2001) القيادة والادارة في عصر العولمة. أبو ظبي: المؤلف.

مفتاح الإنترنت (1997)، الإنترنت آفاق بلا حدود ، مجلة مفتاح الإنترنت ، (رقم العدد غير موجود) ،10-17 .

يماني، محمد عبده (1998). عصر المعلومات وعصارة التعليم. مجلة المعرفة، ع35، صفر.

ينييس وارين: وداعاً للقيادة القديمة ص ص29-58 فيمركز الامارات للدراسات والبحوث والاستراتيجية (2001) القيادة والادارة في عصر العولمة. أبو ظبي: المؤلف.